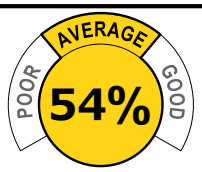
CONFIGURATION AUDIT OF MICROSOFT WINDOWS

Computer:	**ERZA (Domain member - DCIT)**
Operating system:	**Windows Server 2012 R2 Standard (64bit)**
Audit date:	**2016-02-18 15:45**
Checklist:	**Audit Square - std. security/2016b**



Area	Check		Result *)
[BASE] Basic tests	**BASE-01**	*OS version and updates*	Warning
	BASE-02	*Installed software*	Fail
	BASE-03	*Environment variables*	Ok
	BASE-04	*Other operating system settings*	Ok
[SVCS] System services	**SVCS-01**	*Basic configuration of system services*	Fail
	SVCS-02	*Drivers*	Warning
	SVCS-03	*Services and drivers access permissions*	Ok
	SVCS-04	*Service accounts*	Ok
	SVCS-05	*Other programs that run automatically*	Ok
[SECP] Security policy	**SECP-01**	*Passwords and account locking policy*	Fail
	SECP-02	*Security settings*	Fail
	SECP-03	*Audit settings*	Fail
	SECP-04	*Parameters of log files*	Ok
	SECP-05	*Other security settings*	Fail
[USER] User accounts	**USER-01**	*System-wide privileges*	Fail
	USER-02	*Problematic active accounts*	Ok
	USER-03	*Local groups membership*	Fail
	USER-04	*Logon cache*	Ok
[ACLS] Access control	**ACLS-01**	*File system of local drives*	Ok
	ACLS-02	*File access permissions*	Ok
[NETW] Network settings	**NETW-01**	*Global settings*	Warning
	NETW-02	*Problematic open TCP/UDP ports*	Warning
	NETW-03	*System server components configuration*	Fail
	NETW-04	*Shared resources*	Ok

*) You can get to detailed findings by clicking on the check result.

1 COMPUTER ERZA

1.1 [INFO-xx] Assessment info

1.1.1 [INFO-01] Server/workstation

Brief description of the examined computer is shown in the table:

Computer name	ERZA
Domain/workgroup membership	Domain member (DCIT)
Operating system version	6.3 (Windows Server 2012 R2 Standard)
CPU architecture, thread count	x86-64 x 12 (AMD Opteron(tm) Processor 4334)
Installed physical memory size	32.0 GB
HW classification	standard
OS root directory	C:\Windows
OS install date	2014-11-05 20:53
Boot time	2016-02-08 19:49

[Computer ERZA] [Top][Summary][Explanatory notes]

1.1.2 [INFO-02] Data collection

Data collection parameters are listed in the table below:

Collection date	2016-02-18 15:45
Account used	ERZA\SYSTEM
Client version	2.7.5
Data processor version	1.1.3.1

[Computer ERZA] [Top][Summary][Explanatory notes]

1.2 [BASE-xx] Basic tests

1.2.1 [BASE-01] OS version and updates

The check verifies the operating system version, installed service packs and hotfixes and settings of automatic updates service. If the version of the operating system is different from the given value, if the number of installed service pack is less than the specified value, if more than a specified time passed since the last hotfix installation, or if the configuration of automatic updates does not comply with the requirements, the overall result of a check is **FAIL**. Optional parameters allow to fine-tune the behavior of the check.

Check result: OK WITH WARNING.

The values to be verified are listed in the table below. Problematic values are marked in red:

Category	Parameter name	Value	Recommendation
Version	OS Version	WINDOWS 2012 R2 (6.3)	
	Service Pack	SP0	
Hotfixes and patches	Last hotfix installation date	2016-02-08	
Automatic Updates	Service status	Stopped/Manual (Trigger Start)	
	Updates configuration	Configured locally (mode: 3-Download only)	
	Server redirection	--	☹ (local WSUS via encrypted connection (https))

Category	Parameter name	Value	Recommendation
	Status server redirection	--	☹ (local WSUS via encrypted connection (https))

[Computer ERZA] [Top][Summary][Explanatory notes]

1.2.2 [BASE-02] Installed software

The installed software packages are checked against the set of rules. If any installed software does not comply with requirements, the overall result of the check is **FAIL**. Details of instances found are given in the results table.

Note: only the software installed by standard means and recorded in the system installation database is reported.

Check result: FAIL.

Problematic software packages must either be uninstalled or updated to the safe version, as indicated in the column with the recommendation.

The table lists the details of installed software:

Software	Producer	Version	Finding	Recommendation
Audit Square PRO Agent	AuditSquare.com	2.7.5	ok	
Broadcom Drivers and Management Applications	Broadcom Corporation	16.6.7.2	ok	
Dell OpenManage Systems Management Software (64-Bit)	Dell	7.4.0	ok	
GDR 5343 for SQL Server 2012 (KB3045321) (64-bit)	Microsoft Corporation	11.2.5343.0	ok	
HP 3PAR StoreServ Plug-in	Veeam Software AG	8.0.0.817	ok	
HP StoreVirtual Plug-in	Veeam Software AG	8.0.0.817	ok	
Matrox Graphics Software (remove only)	Matrox Graphics Inc.	4.0.1.4	ok	
Microsoft Application Error Reporting	Microsoft Corporation	12.0.6015.5000	ok	
Microsoft Report Viewer 2012 Runtime	Microsoft Corporation	11.1.3452.0	ok	
Microsoft SQL Server 2008 (64-bit)	Microsoft Corporation	(n/a)	ok	
Microsoft SQL Server 2008 Management Studio	Microsoft Corporation	10.0.1600.22	ok	
Microsoft SQL Server 2008 Policies	Microsoft Corporation	10.0.1600.22	ok	
Microsoft SQL Server 2008 R2 (64-bit)	Microsoft Corporation	(n/a)	ok	
Microsoft SQL Server 2008 R2 Native Client	Microsoft Corporation	10.51.2500.0	ok	
Microsoft SQL Server 2008 R2 RsFx Driver	Microsoft Corporation	10.51.2500.0	ok	
Microsoft SQL Server 2008 R2 Setup (English)	Microsoft Corporation	10.51.2500.0	ok	
Microsoft SQL Server 2008 Setup Support Files	Microsoft Corporation	10.1.2731.0	ok	
Microsoft SQL Server 2012 (64-bit)	Microsoft Corporation	(n/a)	ok	
Microsoft SQL Server 2012 (64-bit)	(n/a)	(n/a)	ok	
Microsoft SQL Server 2012 Management Objects (x64)	Microsoft Corporation	11.0.2100.60	ok	
Microsoft SQL Server 2012 Native Client	Microsoft Corporation	11.2.5058.0	ok	
Microsoft SQL Server 2012 RsFx Driver	Microsoft Corporation	11.2.5058.0	ok	

Software	Producer	Version	Finding	Recommendation
Microsoft SQL Server 2012 Setup (English)	Microsoft Corporation	11.2.5343.0	ok	
Microsoft SQL Server 2012 Transact-SQL ScriptDom	Microsoft Corporation	11.2.5058.0	ok	
Microsoft SQL Server Compact 3.5 SP1 English	Microsoft Corporation	3.5.5692.0	ok	
Microsoft SQL Server Compact 3.5 SP1 Query Tools English	Microsoft Corporation	3.5.5692.0	ok	
Microsoft System CLR Types for SQL Server 2012 (x64)	Microsoft Corporation	11.2.5058.0	ok	
Microsoft Visual C++ 2010 x64 Redistributable - 10.0.40219	Microsoft Corporation	10.0.40219	ok	
Microsoft Visual C++ 2010 x86 Redistributable - 10.0.40219	Microsoft Corporation	10.0.40219	ok	
Microsoft Visual Studio Tools for Applications 2.0 - ENU	Microsoft Corporation	9.0.30729	ok	
Microsoft VSS Writer for SQL Server 2012	Microsoft Corporation	11.2.5058.0	ok	
Mozilla Firefox 31.2.0 ESR (x86 en-US)	Mozilla	31.2.0	SW not recommended by profile; installed version vulnerable	consider removing; or at least upgrade
Mozilla Maintenance Service	Mozilla	31.2.0	ok	
NEC Electronics USB 3.0 Host Controller Driver	NEC Electronics Corporation	1.0.19.0	ok	
NetApp Plug-in	Veeam Software AG	8.0.0.817	ok	
Service Pack 1 for SQL Server 2008 R2 (KB2528583) (64-bit)	Microsoft Corporation	10.51.2500.0	ok	
Service Pack 2 for SQL Server 2012 (KB2958429) (64-bit)	Microsoft Corporation	11.2.5058.0	ok	
SQL Server 2008 R2 SP1 Common Files	Microsoft Corporation	10.51.2500.0	ok	
SQL Server 2008 R2 SP1 Database Engine Services	Microsoft Corporation	10.51.2500.0	ok	
SQL Server 2008 R2 SP1 Database Engine Shared	Microsoft Corporation	10.51.2500.0	ok	
SQL Server 2012 Common Files	Microsoft Corporation	11.2.5058.0	ok	
SQL Server 2012 Database Engine Services	Microsoft Corporation	11.2.5058.0	ok	
SQL Server 2012 Database Engine Shared	Microsoft Corporation	11.2.5058.0	ok	
SQL Server Browser for SQL Server 2012	Microsoft Corporation	11.2.5058.0	ok	
Sql Server Customer Experience Improvement Program	Microsoft Corporation	10.50.1600.1	ok	
Sql Server Customer Experience Improvement Program	Microsoft Corporation	11.2.5058.0	ok	
Total Commander 64-bit (Remove or Repair)	Ghisler Software GmbH	8.51a	ok	
Veeam Backup Catalog	Veeam Software AG	8.0.0.817	ok	
Veeam Backup Enterprise Manager	Veeam Software AG	8.0.0.817	ok	
Veeam Backup &	Veeam Software AG	8.0.0.817	ok	

Software	Producer	Version	Finding	Recommendation
Replication				
Veeam Backup & Replication PowerShell SDK	Veeam Software AG	8.0.0.817	ok	
Veeam Backup Transport	Veeam Software AG	8.0.0.2084	ok	
Veeam Backup vPowerNFS	Veeam Software AG	8.0.0.2084	ok	
Veeam Explorer for Microsoft Active Directory	Veeam Software AG	8.0.0.952	ok	
Veeam Explorer for Microsoft Exchange	Veeam Software AG	8.0.0.951	ok	
Veeam Explorer for Microsoft SharePoint	Veeam Software AG	8.0.0.950	ok	
Veeam Explorer for Microsoft SQL Server	Veeam Software AG	8.0.0.953	ok	
Veeam ONE	Veeam Software	8.0.0.1569	ok	
Veeam ONE Business View	Veeam Software	8.0.0.1569	ok	
Veeam ONE Monitor Client	Veeam Software	8.0.0.1569	ok	
Veeam ONE Monitor Server	Veeam Software	8.0.0.1569	ok	
Veeam ONE Reporter Server	Veeam Software	8.0.0.1569	ok	
Veeam ONE Reporter Web	Veeam Software	8.0.0.1569	ok	
WinPcap 4.1.3	Riverbed Technology, Inc.	4.1.0.2980	SW forbidden by profile	remove
Wireshark 1.12.3 (64-bit)	The Wireshark developer community, http://www.wireshark.org	1.12.3	ok	

[Computer ERZA] [Top][Summary][Explanatory notes]

1.2.3 [BASE-03] Environment variables

The check verifies correctness of the settings of several important system environment variables, namely **COMSPEC**, **PATHEXT** and **PATH**. **COMSPEC** must refer to std. command interpreter (cmd.exe). **PATHEXT** must not contain non-default values for the given operating system. The most comprehensive is the testing of the **PATH** variable, which for the successful test outcome must not contain a directory writable by unprivileged users (exceptions can be specified using the check parameters if necessary).

Check result: OK.

These settings must be fixed manually directly on the server/workstation *(Control Panel - System - Advanced System Settings - Environment Variables)*. However, in the case of problematic entries in the **PATH**, the preferred solution is to fix directory permissions (removing the write permissions for unprivileged users and groups).Related link:Setting the PATH

Parameter	Value	Recommendation
PATHEXT	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC	
ComSpec	C:\Windows\system32\cmd.exe	
PATH	C:\Windows\system32	
	C:\Windows	
	C:\Windows\system32\Wbem	
	C:\Windows\system32\WindowsPowerShell\v1.0	
	C:\Program Files\Dell\SysMgt\oma\bin	
	C:\Program Files\Dell\SysMgt\shared\bin	
	C:\Program Files\Dell\SysMgt\idrac	
	C:\Program Files (x86)\Microsoft SQL Server\100\Tools\Binn	
	C:\Program Files\Microsoft SQL Server\100\Tools\Binn	
	C:\Program Files\Microsoft SQL	

Parameter	Value	Recommendation
	Server\100\DTS\Binn	
	C:\Program Files (x86)\Microsoft SQL Server\110\Tools\Binn	
	C:\Program Files\Microsoft SQL Server\110\Tools\Binn	
	C:\Program Files\Microsoft SQL Server\110\DTS\Binn	
	C:\Program Files (x86)\Microsoft SQL Server\100\Tools\Binn\VSShell\Common7\IDE	
	C:\Program Files (x86)\Microsoft SQL Server\100\DTS\Binn	

[Computer ERZA] [Top][Summary][Explanatory notes]

1.2.4 [BASE-04] Other operating system settings

Check verifies the settings of several operating system parameters not included in other chapters. Audited settings include OS loader configuration, the OS response to fatal accidents, time synchronization and automatic login. Individual tests can optionally be turned off by the corresponding check arguments. The details of tests behavior can sometimes be further refined by check arguments as well.

Check result: OK.

The settings tested in this check must usually be adjusted manually directly on the computer without help of Group Policy. Details are beyond the scope of this report, please refer to the operating system manufacturer's documentation. Here only a quick hint on some topics:

- **OS loader** - *Control Panel - System - Advanced System Settings - Startup and Recovery*, or command line tools *(bootcfg, bcdedit)* (related link: DEP configuration);
- **Crash control** - *Control Panel - System - Advanced System Settings - Startup and Recovery* (related link: Crash control);
- **Automatic logon** - utility *netplwiz* (Windows Vista and higher), or direct modification of the registry, the key *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon* (related link: Disabling autologon).

Component	Parameter name	Value	Recommendation
OS clock	Time synchronization	Ok	
Winlogon	Automatic logon	Disabled	

[Computer ERZA] [Top][Summary][Explanatory notes]

1.3 [SVCS-xx] System services

1.3.1 [SVCS-01] Basic configuration of system services

The check evaluates the configuration of system services, according to the specified set of rules. Following service attributes are verified: the current state of the service, its start mode, path to the binary image, image maker and image signer. With a set of custom rules blacklist-type checking can be performed (ban on the operation of certain services) as well as whitelist (allowing only the listed services) or requestlist (request the mandatory operation of certain services).

Check result: FAIL.

Security issues detected in this chapter may be fixed in different ways depending on the problem found: by removing or disabling the problematic services, adding them to the set of rules (whitelist), or changing the services' starting parameters. The latter could be performed locally (eg. by using mmc snap-in Services), but the use of Group Policy is recommended for efficiency reasons. GPO path to the settings is *Computer Configuration(/Policies)/Windows Settings/Security Settings/System Services*. However, caution is required when preparing the GPO; it should set only the service starting mode, but not service access permissions.

The table lists the system services with configuration or current state not matching the requirements:

Service	Status	Exe	Company	Signer	Recommendation
AeLookupSvc (Application Experience)	Stopped/Manual (Trigger Start)	(svchost) C:\Windows\system32\aelupsvc.dll	Microsoft Corporation	Microsoft Windows	
ALG (Application Layer Gateway Service)	Stopped/Manual	C:\Windows\system32\alg.exe	Microsoft Corporation	Microsoft Windows	
AppHostSvc (Application Host Helper Service)	Running/Auto	(svchost) C:\Windows\system32\inetsrv\apphostsvc.dll	Microsoft Corporation	Microsoft Windows	
AppIDSvc (Application Identity)	Stopped/Manual (Trigger Start)	(svchost) C:\Windows\system32\appidsvc.dll	Microsoft Corporation	Microsoft Windows	
Appinfo (Application Information)	Running/Manual (Trigger Start)	(svchost) C:\Windows\system32\appinfo.dll	Microsoft Corporation	Microsoft Windows	
AppMgmt (Application Management)	Stopped/Manual	(svchost) C:\Windows\system32\appmgmts.dll	Microsoft Corporation	Microsoft Windows	
AppReadiness (App Readiness)	Stopped/Manual	(svchost) C:\Windows\system32\AppReadiness.dll	Microsoft Corporation	Microsoft Windows	
AppXSvc (AppX Deployment Service (AppXSVC))	Stopped/Manual	(svchost) C:\Windows\system32\appxdeploymentserver.dll	Microsoft Corporation	Microsoft Windows	
aspnet_state (ASP.NET State Service)	Stopped/Manual	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_state.exe	Microsoft Corporation	Microsoft Windows	
AudioEndpointBuilder (Windows Audio Endpoint Builder)	Running/Manual	(svchost) C:\Windows\system32\audioendpointbuilder.dll	Microsoft Corporation	Microsoft Windows	☹ adjust the starting of the service (disabled)
Audiosrv (Windows Audio)	Running/Auto	(svchost) C:\Windows\system32\audiosrv.dll	Microsoft Corporation	Microsoft Windows	☹ adjust the starting of the service (disabled)
BFE (Base Filtering Engine)	Running/Auto	(svchost) C:\Windows\system32\BFE.DLL	Microsoft Corporation	Microsoft Windows	
BITS (Background Intelligent Transfer Service)	Running/Manual	(svchost) C:\Windows\system32\qmgr.dll	Microsoft Corporation	Microsoft Windows	
BrokerInfrastructure (Background Tasks Infrastructure Service)	Running/Auto	(svchost) C:\Windows\system32\bisrv.dll	Microsoft Corporation	Microsoft Windows	
Browser (Computer Browser)	Stopped/Disabled	(svchost) C:\Windows\system32\browser.dll	Microsoft Corporation	Microsoft Windows	
CertPropSvc (Certificate Propagation)	Running/Manual	(svchost) C:\Windows\system32\certprop.dll	Microsoft Corporation	Microsoft Windows	
COMSysApp (COM+ System Application)	Stopped/Manual	C:\Windows\system32\dllhost.exe	Microsoft Corporation	Microsoft Windows	
CryptSvc (Cryptographic Services)	Running/Auto	(svchost) C:\Windows\system32\cryptsvc.dll	Microsoft Corporation	Microsoft Windows	
dcevt64 (DSM SA Event Manager)	Running/Auto	C:\Program Files\Dell\SysMgt\dataeng\bin\dsm_sa_eventmgr64.exe	Dell Inc.	Dell Inc.	
DcomLaunch (DCOM Server Process Launcher)	Running/Auto	(svchost) C:\Windows\system32\rpcss.dll	Microsoft Corporation	Microsoft Windows	
dcstor64 (DSM SA	Running/Auto	C:\Program	Dell Inc.	Dell Inc.	

Service	Status	Exe	Company	Signer	Recommendation
Data Manager)		Files\Dell\SysMgt\dataeng\bin\dsm_sa_datamgr64.exe			
ddpsvc (Data Deduplication Service)	Running/Manual	(svchost) C:\Windows\system32\ddpsvc.dll	Microsoft Corporation	Microsoft Windows	
ddpvssvc (Data Deduplication Volume Shadow Copy Service)	Running/Auto	(svchost) C:\Windows\system32\ddpvssvc.dll	Microsoft Corporation	Microsoft Windows	
defragsvc (Optimize drives)	Stopped/Manual	(svchost) C:\Windows\system32\defragsvc.dll	Microsoft Corporation	Microsoft Windows	
DeviceAssociationService (Device Association Service)	Stopped/Manual (Trigger Start)	(svchost) C:\Windows\system32\das.dll	Microsoft Corporation	Microsoft Windows	
DeviceInstall (Device Install Service)	Stopped/Manual (Trigger Start)	(svchost) C:\Windows\system32\umpnpmgr.dll	Microsoft Corporation	Microsoft Windows	
Dhcp (DHCP Client)	Running/Auto	(svchost) C:\Windows\system32\dhcpcore.dll	Microsoft Corporation	Microsoft Windows	
DiagTrack (Diagnostics Tracking Service)	Running/Auto	(svchost) C:\Windows\system32\diagtrack.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
Dnscache (DNS Client)	Running/Auto (Trigger Start)	(svchost) C:\Windows\system32\dnsrslvr.dll	Microsoft Corporation	Microsoft Windows	
dot3svc (Wired AutoConfig)	Stopped/Manual	(svchost) C:\Windows\system32\dot3svc.dll	Microsoft Corporation	Microsoft Windows	
DPS (Diagnostic Policy Service)	Running/Auto (Delayed)	(svchost) C:\Windows\system32\dps.dll	Microsoft Corporation	Microsoft Windows	
DsmSvc (Device Setup Manager)	Stopped/Manual (Trigger Start)	(svchost) C:\Windows\system32\DeviceSetupManager.dll	Microsoft Corporation	Microsoft Windows	
Eaphost (Extensible Authentication Protocol)	Stopped/Manual	(svchost) C:\Windows\system32\eapsvc.dll	Microsoft Corporation	Microsoft Windows	
EFS (Encrypting File System (EFS))	Stopped/Manual (Trigger Start)	C:\Windows\system32\lsass.exe	Microsoft Corporation	Microsoft Windows	
EventLog (Windows Event Log)	Running/Auto	(svchost) C:\Windows\system32\wevtsvc.dll	Microsoft Corporation	Microsoft Windows	
EventSystem (COM+ Event System)	Running/Auto	(svchost) C:\Windows\system32\es.dll	Microsoft Corporation	Microsoft Windows	
fdPHost (Function Discovery Provider Host)	Stopped/Manual	(svchost) C:\Windows\system32\fdPHost.dll	Microsoft Corporation	Microsoft Windows	
FDResPub (Function Discovery Resource Publication)	Stopped/Manual	(svchost) C:\Windows\system32\FDResPub.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
FontCache (Windows Font Cache Service)	Running/Auto	(svchost) C:\Windows\system32\FntCache.dll	Microsoft Corporation	Microsoft Windows	
FontCache3.0.0.0 (Windows Presentation Foundation Font Cache 3.0.0.0)	Stopped/Manual	C:\Windows\Microsoft.Net\Framework64\v3.0\WPF\PresentationFontCache.exe	Microsoft Corporation	Microsoft Windows	
gpsvc (Group Policy Client)	Running/Auto (Trigger Start)	(svchost) C:\Windows\system32\gpsvc.dll	Microsoft Corporation	Microsoft Windows	

Service	Status	Exe	Company	Signer	Recommendation
hidserv (Human Interface Device Service)	Running/Manual (Trigger Start)	(svchost) C:\Windows\system32\hidserv.dll	Microsoft Corporation	Microsoft Windows	☹ adjust the starting of the service (disabled)
hkmsvc (Health Key and Certificate Management)	Stopped/Manual	(svchost) C:\Windows\system32\KMSVC.DLL	Microsoft Corporation	Microsoft Windows	
IEEtwCollectorService (Internet Explorer ETW Collector Service)	Stopped/Manual	C:\Windows\system32\IEEtwCollector.exe	Microsoft Corporation	Microsoft Windows	
IKEEXT (IKE and AuthIP IPsec Keying Modules)	Running/Auto (Trigger Start)	(svchost) C:\Windows\system32\IKEEXT.DLL	Microsoft Corporation	Microsoft Windows	
iphlpsvc (IP Helper)	Running/Auto	(svchost) C:\Windows\system32\iphlpsvc.dll	Microsoft Corporation	Microsoft Windows	
KeyIso (CNG Key Isolation)	Stopped/Manual (Trigger Start)	C:\Windows\system32\lsass.exe	Microsoft Corporation	Microsoft Windows	
KPSSVC (KDC Proxy Server service (KPS))	Stopped/Manual	(svchost) C:\Windows\system32\kpssvc.dll	Microsoft Corporation	Microsoft Windows	
KtmRm (KtmRm for Distributed Transaction Coordinator)	Stopped/Manual (Trigger Start)	(svchost) C:\Windows\system32\msdtckrm.dll	Microsoft Corporation	Microsoft Windows	
LanmanServer (Server)	Running/Auto	(svchost) C:\Windows\system32\srvsvc.dll	Microsoft Corporation	Microsoft Windows	
LanmanWorkstation (Workstation)	Running/Auto	(svchost) C:\Windows\system32\wkssvc.dll	Microsoft Corporation	Microsoft Windows	
lltdsvc (Link-Layer Topology Discovery Mapper)	Stopped/Manual	(svchost) C:\Windows\system32\lltdsvc.dll	Microsoft Corporation	Microsoft Windows	
lmhosts (TCP/IP NetBIOS Helper)	Running/Auto (Trigger Start, Trigger Stop)	(svchost) C:\Windows\system32\lmhsvc.dll	Microsoft Corporation	Microsoft Windows	
LSM (Local Session Manager)	Running/Auto	(svchost) C:\Windows\system32\lsm.dll	Microsoft Corporation	Microsoft Windows	
MMCSS (Multimedia Class Scheduler)	Running/Manual	(svchost) C:\Windows\system32\mmcss.dll	Microsoft Corporation	Microsoft Windows	☹ adjust the starting of the service (disabled)
MozillaMaintenance (Mozilla Maintenance Service)	Stopped/Manual	C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe	Mozilla Foundation	Mozilla Corporation	
MpsSvc (Windows Firewall)	Running/Auto	(svchost) C:\Windows\system32\MPSSVC.dll	Microsoft Corporation	Microsoft Windows	
MSDTC (Distributed Transaction Coordinator)	Running/Auto (Delayed)	C:\Windows\system32\msdtc.exe	Microsoft Corporation	Microsoft Windows	
MSiSCSI (Microsoft iSCSI Initiator Service)	Stopped/Manual	(svchost) C:\Windows\system32\iscsiexe.dll	Microsoft Corporation	Microsoft Windows	
msiserver (Windows Installer)	Stopped/Manual	C:\Windows\system32\msiexec.exe	Microsoft Corporation	Microsoft Windows	
MSSQL$VEEAMSQL2008R2 (SQL Server (VEEAMSQL2008R2))	Running/Auto	C:\Program Files\Microsoft SQL Server\MSSQL10_50.VEEAMSQL2008R2\MSSQL\Binn\sqlservr.exe	Microsoft Corporation	Microsoft Corporation	

Service	Status	Exe	Company	Signer	Recommendation
MSSQL$VEEAMSQL2012 (SQL Server (VEEAMSQL2012))	Running/Auto	C:\Program Files\Microsoft SQL Server\MSSQL11.VEEAMSQL2012\MSSQL\Binn\sqlservr.exe	Microsoft Corporation	Microsoft Corporation	
MSSQLServerADHelper100 (SQL Active Directory Helper Service)	Stopped/Disabled	C:\Program Files\Microsoft SQL Server\100\Shared\sqladhlp.exe	Microsoft Corporation	Microsoft Corporation	
napagent (Network Access Protection Agent)	Stopped/Manual	(svchost) C:\Windows\system32\QAGENTRT.DLL	Microsoft Corporation	Microsoft Windows	
NcaSvc (Network Connectivity Assistant)	Stopped/Manual (Trigger Start, Trigger Stop)	(svchost) C:\Windows\system32\NcaSvc.dll	Microsoft Corporation	Microsoft Windows	
Netlogon (Netlogon)	Running/Auto	C:\Windows\system32\lsass.exe	Microsoft Corporation	Microsoft Windows	
Netman (Network Connections)	Running/Manual	(svchost) C:\Windows\system32\netman.dll	Microsoft Corporation	Microsoft Windows	
netprofm (Network List Service)	Running/Manual	(svchost) C:\Windows\system32\netprofmsvc.dll	Microsoft Corporation	Microsoft Windows	
NetTcpPortSharing (Net.Tcp Port Sharing Service)	Stopped/Disabled	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe	Microsoft Corporation	Microsoft Windows	
NlaSvc (Network Location Awareness)	Running/Auto	(svchost) C:\Windows\system32\nlasvc.dll	Microsoft Corporation	Microsoft Windows	
nsi (Network Store Interface Service)	Running/Auto	(svchost) C:\Windows\system32\nsisvc.dll	Microsoft Corporation	Microsoft Windows	
omsad (DSM SA Shared Services)	Running/Auto	C:\Program Files\Dell\SysMgt\oma\bin\dsm_om_shrsvc64.exe	Dell Inc.	Dell Inc.	
PerfHost (Performance Counter DLL Host)	Stopped/Manual	C:\Windows\SysWOW64\perfhost.exe	Microsoft Corporation	Microsoft Windows	
pla (Performance Logs & Alerts)	Stopped/Manual	(svchost) C:\Windows\system32\pla.dll	Microsoft Corporation	Microsoft Windows	
PlugPlay (Plug and Play)	Running/Manual	(svchost) C:\Windows\system32\umpnpmgr.dll	Microsoft Corporation	Microsoft Windows	
PolicyAgent (IPsec Policy Agent)	Running/Manual (Trigger Start)	(svchost) C:\Windows\system32\IPSECSVC.DLL	Microsoft Corporation	Microsoft Windows	
Power (Power)	Running/Auto	(svchost) C:\Windows\system32\umpo.dll	Microsoft Corporation	Microsoft Windows	
PrintNotify (Printer Extensions and Notifications)	Stopped/Manual	(svchost) C:\Windows\system32\spool\drivers\x64\3\PrintConfig.dll	Microsoft Corporation	Microsoft Windows	
ProfSvc (User Profile Service)	Running/Auto	(svchost) C:\Windows\system32\profsvc.dll	Microsoft Corporation	Microsoft Windows	
RasAuto (Remote Access Auto Connection Manager)	Stopped/Manual	(svchost) C:\Windows\system32\rasauto.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
RasMan (Remote Access Connection Manager)	Stopped/Manual	(svchost) C:\Windows\system32\rasmans.dll	Microsoft Corporation	Microsoft Windows	

Service	Status	Exe	Company	Signer	Recommendation
RemoteAccess (Routing and Remote Access)	Stopped/Disabled	(svchost) C:\Windows\system32\mprdim.dll	Microsoft Corporation	Microsoft Windows	
RemoteRegistry (Remote Registry)	Stopped/Auto (Trigger Start)	(svchost) C:\Windows\system32\regsvc.dll	Microsoft Corporation	Microsoft Windows	
rpcapd (Remote Packet Capture Protocol v.0 (experimental))	Stopped/Disabled	C:\Program Files (x86)\WinPcap\rpcapd.exe	Riverbed Technology, Inc.	Riverbed Technology, Inc.	
RpcEptMapper (RPC Endpoint Mapper)	Running/Auto	(svchost) C:\Windows\system32\RpcEpMap.dll	Microsoft Corporation	Microsoft Windows	
RpcLocator (Remote Procedure Call (RPC) Locator)	Stopped/Manual	C:\Windows\system32\Locator.exe	Microsoft Corporation	Microsoft Windows	
RpcSs (Remote Procedure Call (RPC))	Running/Auto	(svchost) C:\Windows\system32\rpcss.dll	Microsoft Corporation	Microsoft Windows	
RSoPProv (Resultant Set of Policy Provider)	Stopped/Manual	C:\Windows\system32\rsopprov.exe	Microsoft Corporation	Microsoft Windows	
sacsvr (Special Administration Console Helper)	Stopped/Manual	(svchost) C:\Windows\system32\sacsvr.dll	Microsoft Corporation	Microsoft Windows	
SamSs (Security Accounts Manager)	Running/Auto	C:\Windows\system32\lsass.exe	Microsoft Corporation	Microsoft Windows	
SCardSvr (Smart Card)	Stopped/Disabled	(svchost) C:\Windows\system32\SCardSvr.dll	Microsoft Corporation	Microsoft Windows	
ScDeviceEnum (Smart Card Device Enumeration Service)	Stopped/Manual (Trigger Start)	(svchost) C:\Windows\system32\scdeviceenum.dll	Microsoft Corporation	Microsoft Windows	
Schedule (Task Scheduler)	Running/Auto	(svchost) C:\Windows\system32\schedsvc.dll	Microsoft Corporation	Microsoft Windows	
SCPolicySvc (Smart Card Removal Policy)	Stopped/Manual	(svchost) C:\Windows\system32\certprop.dll	Microsoft Corporation	Microsoft Windows	
seclogon (Secondary Logon)	Stopped/Manual	(svchost) C:\Windows\system32\seclogon.dll	Microsoft Corporation	Microsoft Windows	
SENS (System Event Notification Service)	Running/Auto	(svchost) C:\Windows\system32\Sens.dll	Microsoft Corporation	Microsoft Windows	
Server Administrator (DSM SA Connection Service)	Running/Auto	C:\Program Files\Dell\SysMgt\oma\bin\dsm_om_connsvc64.exe	Dell Inc.	Dell Inc.	
SessionEnv (Remote Desktop Configuration)	Running/Manual	(svchost) C:\Windows\system32\SessEnv.dll	Microsoft Corporation	Microsoft Windows	
SharedAccess (Internet Connection Sharing (ICS))	Stopped/Disabled	(svchost) C:\Windows\system32\ipnathlp.dll	Microsoft Corporation	Microsoft Windows	
ShellHWDetection (Shell Hardware Detection)	Running/Auto	(svchost) C:\Windows\system32\shsvcs.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
smphost (Microsoft Storage Spaces SMP)	Stopped/Manual	(svchost) C:\Windows\system32\smphost.dll	Microsoft Corporation	Microsoft Windows	
SNMPTRAP (SNMP Trap)	Stopped/Manual	C:\Windows\system32\snmptrap.exe	Microsoft Corporation	Microsoft Windows	
Spooler (Print Spooler)	Running/Auto	C:\Windows\system32\spoolsv.exe	Microsoft Corporation	Microsoft Windows	

Service	Status	Exe	Company	Signer	Recommendation
sppsvc (Software Protection)	Stopped/Auto (Delayed, Trigger Start)	C:\Windows\system32\sppsvc.exe	Microsoft Corporation	Microsoft Windows	
SQLAgent$VEEAMSQL2008R2 (SQL Server Agent (VEEAMSQL2008R2))	Stopped/Disabled	C:\Program Files\Microsoft SQL Server\MSSQL10_50.VEEAMSQL2008R2\MSSQL\Binn\SQLAGENT.EXE	Microsoft Corporation	Microsoft Corporation	
SQLAgent$VEEAMSQL2012 (SQL Server Agent (VEEAMSQL2012))	Stopped/Disabled	C:\Program Files\Microsoft SQL Server\MSSQL11.VEEAMSQL2012\MSSQL\Binn\SQLAGENT.EXE	Microsoft Corporation	Microsoft Corporation	
SQLBrowser (SQL Server Browser)	Running/Auto	C:\Program Files (x86)\Microsoft SQL Server\90\Shared\sqlbrowser.exe	Microsoft Corporation	Microsoft Corporation	
SQLWriter (SQL Server VSS Writer)	Running/Auto	C:\Program Files\Microsoft SQL Server\90\Shared\sqlwriter.exe	Microsoft Corporation	Microsoft Corporation	
SSDPSRV (SSDP Discovery)	Stopped/Disabled	(svchost) C:\Windows\system32\ssdpsrv.dll	Microsoft Corporation	Microsoft Windows	
SstpSvc (Secure Socket Tunneling Protocol Service)	Stopped/Manual	(svchost) C:\Windows\system32\sstpsvc.dll	Microsoft Corporation	Microsoft Windows	
svsvc (Spot Verifier)	Stopped/Manual (Trigger Start)	(svchost) C:\Windows\system32\svsvc.dll	Microsoft Corporation	Microsoft Windows	
swprv (Microsoft Software Shadow Copy Provider)	Stopped/Manual	(svchost) C:\Windows\system32\swprv.dll	Microsoft Corporation	Microsoft Windows	
SysMain (Superfetch)	Stopped/Manual	(svchost) C:\Windows\system32\sysmain.dll	Microsoft Corporation	Microsoft Windows	
SystemEventsBroker (System Events Broker)	Running/Auto (Trigger Start)	(svchost) C:\Windows\system32\systemeventsbrokerserver.dll	Microsoft Corporation	Microsoft Windows	
TapiSrv (Telephony)	Stopped/Manual	(svchost) C:\Windows\system32\tapisrv.dll	Microsoft Corporation	Microsoft Windows	
TermService (Remote Desktop Services)	Running/Manual	(svchost) C:\Windows\system32\termsrv.dll	Microsoft Corporation	Microsoft Windows	
Themes (Themes)	Running/Auto	(svchost) C:\Windows\system32\themeservice.dll	Microsoft Corporation	Microsoft Windows	☹ adjust the starting of the service (disabled)
THREADORDER (Thread Ordering Server)	Stopped/Manual	(svchost) C:\Windows\system32\mmcss.dll	Microsoft Corporation	Microsoft Windows	
TieringEngineService (Storage Tiers Management)	Stopped/Manual	C:\Windows\system32\TieringEngineService.exe	Microsoft Corporation	Microsoft Windows	
TrkWks (Distributed Link Tracking Client)	Running/Auto	(svchost) C:\Windows\system32\trkwks.dll	Microsoft Corporation	Microsoft Windows	☹ adjust the starting of the service (disabled)
TrustedInstaller (Windows Modules Installer)	Stopped/Manual	C:\Windows\servicing\TrustedInstaller.exe	Microsoft Corporation	Microsoft Windows	
UALSVC (User Access Logging Service)	Running/Auto (Delayed)	(svchost) C:\Windows\system32	Microsoft Corporation	Microsoft Windows	

Service	Status	Exe	Company	Signer	Recommendation
		\ualsvc.dll			
UI0Detect (Interactive Services Detection)	Stopped/Manual	C:\Windows\system32\UI0Detect.exe	Microsoft Corporation	Microsoft Windows	
UmRdpService (Remote Desktop Services UserMode Port Redirector)	Running/Manual	(svchost) C:\Windows\system32\umrdp.dll	Microsoft Corporation	Microsoft Windows	
upnphost (UPnP Device Host)	Stopped/Disabled	(svchost) C:\Windows\system32\upnphost.dll	Microsoft Corporation	Microsoft Windows	
VaultSvc (Credential Manager)	Stopped/Manual	C:\Windows\system32\lsass.exe	Microsoft Corporation	Microsoft Windows	
vds (Virtual Disk)	Stopped/Manual	C:\Windows\system32\vds.exe	Microsoft Corporation	Microsoft Windows	
Veeam Backup and Replication Service (Veeam Backup Service)	Running/Auto (Delayed)	C:\Program Files\Veeam\Backup and Replication\Backup\Veeam.Backup.Service.exe	Veeam Software AG	<no signature>	☹ check the origin of the service
Veeam Backup Catalog Data Service (Veeam Backup Catalog Data Service)	Running/Auto (Delayed)	C:\Program Files\Veeam\Backup and Replication\Backup Catalog\Veeam.Backup.CatalogDataService.exe	Veeam Software AG	<no signature>	☹ check the origin of the service
Veeam Backup Enterprise Manager (Veeam Backup Enterprise Manager)	Running/Auto (Delayed)	C:\Program Files\Veeam\Backup and Replication\EnterpriseManager\Veeam.Backup.EnterpriseService.exe	Veeam Software AG	<no signature>	☹ check the origin of the service
Veeam Backup Restful API (Veeam Backup Restful API)	Running/Auto (Delayed)	C:\Program Files\Veeam\Backup and Replication\EnterpriseManager\Veeam.Backup.Enterprise.RestAPIService.exe	Veeam Software AG	<no signature>	☹ check the origin of the service
VeeamCloudSvc (Veeam Cloud Connect Service)	Running/Auto (Delayed)	C:\Program Files\Veeam\Backup and Replication\Backup\Veeam.Backup.CloudService.exe	Veeam Software AG	<no signature>	☹ check the origin of the service
VeeamDCS (Veeam ONE Monitor Server)	Running/Auto	C:\Program Files\Veeam\Veeam ONE\Veeam ONE Monitor Server\VeeamDCS.exe	Veeam Software AG	<no signature>	☹ check the origin of the service
VeeamDeploymentService (Veeam Installer Service)	Running/Auto	C:\Program Files\Veeam\Backup and Replication\Backup\VeeamDeploymentSvc.exe	Veeam Software AG	<no signature>	☹ check the origin of the service
VeeamNFSSvc (Veeam vPower NFS Service)	Running/Auto	C:\Program Files (x86)\Veeam\vPower NFS\VeeamNFSSvc.exe	Veeam Software AG	<no signature>	☹ check the origin of the service
VeeamRSS (Veeam ONE Reporter Server)	Running/Auto (Delayed)	C:\Program Files\Veeam\Veeam	Veeam Software AG	<no signature>	☹ check the origin of the service

Service	Status	Exe	Company	Signer	Recommendation
		ONE\Veeam ONE Reporter Server\SchedulingService.exe			
VeeamTransportSvc (Veeam Data Mover Service)	Running/Auto	C:\Program Files (x86)\Veeam\Backup Transport\VeeamTransportSvc.exe	Veeam Software AG	<no signature>	☹ check the origin of the service
vmicguestinterface (Hyper-V Guest Service Interface)	Stopped/Manual (Trigger Start)	(svchost) C:\Windows\system32\icsvc.dll	Microsoft Corporation	Microsoft Windows	
vmicheartbeat (Hyper-V Heartbeat Service)	Stopped/Manual (Trigger Start)	(svchost) C:\Windows\system32\icsvc.dll	Microsoft Corporation	Microsoft Windows	
vmickvpexchange (Hyper-V Data Exchange Service)	Stopped/Manual (Trigger Start)	(svchost) C:\Windows\system32\icsvc.dll	Microsoft Corporation	Microsoft Windows	
vmicrdv (Hyper-V Remote Desktop Virtualization Service)	Stopped/Manual (Trigger Start)	(svchost) C:\Windows\system32\icsvc.dll	Microsoft Corporation	Microsoft Windows	
vmicshutdown (Hyper-V Guest Shutdown Service)	Stopped/Manual (Trigger Start)	(svchost) C:\Windows\system32\icsvc.dll	Microsoft Corporation	Microsoft Windows	
vmictimesync (Hyper-V Time Synchronization Service)	Stopped/Manual (Trigger Start)	(svchost) C:\Windows\system32\icsvc.dll	Microsoft Corporation	Microsoft Windows	
vmicvss (Hyper-V Volume Shadow Copy Requestor)	Stopped/Manual (Trigger Start)	(svchost) C:\Windows\system32\icsvc.dll	Microsoft Corporation	Microsoft Windows	
VSS (Volume Shadow Copy)	Stopped/Manual	C:\Windows\system32\VSSVC.exe	Microsoft Corporation	Microsoft Windows	
W32Time (Windows Time)	Running/Manual (Trigger Start, Trigger Stop)	(svchost) C:\Windows\system32\w32time.dll	Microsoft Corporation	Microsoft Windows	
w3logsvc (W3C Logging Service)	Stopped/Manual	(svchost) C:\Windows\system32\inetsrv\w3logsvc.dll	Microsoft Corporation	Microsoft Windows	
W3SVC (World Wide Web Publishing Service)	Running/Auto	(svchost) C:\Windows\system32\inetsrv\iisw3adm.dll	Microsoft Corporation	Microsoft Windows	
WAS (Windows Process Activation Service)	Running/Manual	(svchost) C:\Windows\system32\inetsrv\iisw3adm.dll	Microsoft Corporation	Microsoft Windows	
wbengine (Block Level Backup Engine Service)	Stopped/Manual	C:\Windows\system32\wbengine.exe	Microsoft Corporation	Microsoft Windows	
Wcmsvc (Windows Connection Manager)	Running/Auto (Trigger Start)	(svchost) C:\Windows\system32\wcmsvc.dll	Microsoft Corporation	Microsoft Windows	
WcsPlugInService (Windows Color System)	Stopped/Manual	(svchost) C:\Windows\system32\WcsPlugInService.dll	Microsoft Corporation	Microsoft Windows	
WdiServiceHost (Diagnostic Service Host)	Stopped/Manual	(svchost) C:\Windows\system32\wdi.dll	Microsoft Corporation	Microsoft Windows	
WdiSystemHost (Diagnostic System Host)	Stopped/Manual	(svchost) C:\Windows\system32\wdi.dll	Microsoft Corporation	Microsoft Windows	
Wecsvc (Windows Event Collector)	Stopped/Manual	(svchost) C:\Windows\system32\wecsvc.dll	Microsoft Corporation	Microsoft Windows	
WEPHOSTSVC (Windows Encryption Provider Host Service)	Stopped/Manual (Trigger Start)	(svchost) C:\Windows\system32\wephostsvc.dll	Microsoft Corporation	Microsoft Windows	

Service	Status	Exe	Company	Signer	Recommendation
wercplsupport (Problem Reports and Solutions Control Panel Support)	Stopped/Manual	(svchost) C:\Windows\system32\wercplsupport.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
WerSvc (Windows Error Reporting Service)	Stopped/Manual (Trigger Start)	(svchost) C:\Windows\system32\wersvc.dll	Microsoft Corporation	Microsoft Windows	
WinHttpAutoProxySvc (WinHTTP Web Proxy Auto-Discovery Service)	Stopped/Manual	(svchost) C:\Windows\system32\winhttp.dll	Microsoft Corporation	Microsoft Windows	
Winmgmt (Windows Management Instrumentation)	Running/Auto	(svchost) C:\Windows\system32\wbem\WMIsvc.dll	Microsoft Corporation	Microsoft Windows	
WinRM (Windows Remote Management (WS-Management))	Running/Auto	(svchost) C:\Windows\system32\WsmSvc.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
wmiApSrv (WMI Performance Adapter)	Stopped/Manual	C:\Windows\system32\wbem\WmiApSrv.exe	Microsoft Corporation	Microsoft Windows	
WPDBusEnum (Portable Device Enumerator Service)	Stopped/Manual (Trigger Start)	(svchost) C:\Windows\system32\wpdbusenum.dll	Microsoft Corporation	Microsoft Windows	
WSService (Windows Store Service (WSService))	Stopped/Manual (Trigger Start)	(svchost) C:\Windows\system32\WSService.dll	Microsoft Corporation	Microsoft Windows	adjust the starting of the service (disabled)
wuauserv (Windows Update)	Stopped/Manual (Trigger Start)	(svchost) C:\Windows\system32\wuaueng.dll	Microsoft Corporation	Microsoft Windows	
wudfsvc (Windows Driver Foundation - User-mode Driver Framework)	Stopped/Manual (Trigger Start)	(svchost) C:\Windows\system32\WUDFSvc.dll	Microsoft Corporation	Microsoft Windows	

[Computer ERZA] [Top][Summary][Explanatory notes]

1.3.2 [SVCS-02] Drivers

The check evaluates the configuration of system drivers, according to the specified set of rules. Following driver attributes are verified: the current state of the driver, its start mode, path to the binary image, image maker and image signer. With a set of custom rules blacklist-type checking can be performed (ban on the operation of certain drivers) as well as whitelist (allowing only the listed drivers) or requestlist (request the mandatory operation of certain drivers).

Check result: OK WITH WARNING.

Fixing of security issues detected in this chapter used to be rather problematic, the driver usually can only be disabled or completely removed, or perhaps updated to newer version.

The table lists the system drivers with configuration or current state not matching the requirements:

Driver	Status	Exe	Company	Signer	Recommendation
1394ohci (1394 OHCI Compliant Host Controller)	Stopped/Disabled	C:\Windows\system32\drivers\1394ohci.sys	Microsoft Corporation	Microsoft Windows	
3ware (3ware)	Stopped/Manual	C:\Windows\system32\drivers\3ware.sys	LSI	Microsoft Windows	
ACPI (Microsoft ACPI Driver)	Running/Boot	C:\Windows\system32\drivers\acpi.sys	Microsoft Corporation	Microsoft Windows	
acpiex (Microsoft ACPIEx Driver)	Running/Boot	C:\Windows\system32\drivers\acpiex.sys	Microsoft Corporation	Microsoft Windows	
acpipagr (ACPI Processor Aggregator Driver)	Stopped/Manual	C:\Windows\system32\drivers\acpipagr.sys	Microsoft Corporation	Microsoft Windows	
AcpiPmi (ACPI Power Meter Driver)	Running/Manual	C:\Windows\system32\drivers\acpipmi.sys	Microsoft Corporation	Microsoft Windows	
acpitime (ACPI Wake	Stopped/Manual	C:\Windows\system32	Microsoft Corporation	Microsoft Windows	

Driver	Status	Exe	Company	Signer	Recommendation
Alarm Driver)		\drivers\acpitime.sys			
ADP80XX (ADP80XX)	Stopped/Manual	C:\Windows\system32\drivers\adp80xx.sys	PMC-Sierra	Microsoft Windows	
AFD (Ancillary Function Driver for Winsock)	Running/System	C:\Windows\system32\drivers\afd.sys	Microsoft Corporation	Microsoft Windows	
agp440 (Intel AGP Bus Filter)	Stopped/Manual	C:\Windows\system32\drivers\AGP440.sys	Microsoft Corporation	Microsoft Windows	
ahcache (Application Compatibility Cache)	Running/System	C:\Windows\system32\drivers\ahcache.sys	Microsoft Corporation	Microsoft Windows	
AmdK8 (AMD K8 Processor Driver)	Stopped/Manual	C:\Windows\system32\drivers\amdk8.sys	Microsoft Corporation	Microsoft Windows	
AmdPPM (AMD Processor Driver)	Running/Manual	C:\Windows\system32\drivers\amdppm.sys	Microsoft Corporation	Microsoft Windows	
amdsata (amdsata)	Stopped/Manual	C:\Windows\system32\drivers\amdsata.sys	Advanced Micro Devices	Microsoft Windows	
amdsbs (amdsbs)	Stopped/Manual	C:\Windows\system32\drivers\amdsbs.sys	AMD Technologies Inc.	Microsoft Windows	
amdxata (amdxata)	Stopped/Manual	C:\Windows\system32\drivers\amdxata.sys	Advanced Micro Devices	Microsoft Windows	
AppID (AppID Driver)	Stopped/Manual	C:\Windows\system32\drivers\appid.sys	Microsoft Corporation	Microsoft Windows	
arcsas (Adaptec SAS/SATA-II RAID Storport's Miniport Driver)	Stopped/Manual	C:\Windows\system32\drivers\arcsas.sys	PMC-Sierra, Inc.	Microsoft Windows	
AsyncMac (RAS Asynchronous Media Driver)	Stopped/Manual	C:\Windows\system32\drivers\asyncmac.sys	Microsoft Corporation	Microsoft Windows	
atapi (IDE Channel)	Stopped/Manual	C:\Windows\system32\drivers\atapi.sys	Microsoft Corporation	Microsoft Windows	
b06bdrv (Broadcom NetXtreme II VBD)	Running/Boot	C:\Windows\system32\drivers\bxvbda.sys	Broadcom Corporation	Broadcom Corporation	
BasicDisplay (BasicDisplay)	Running/System	C:\Windows\system32\drivers\BasicDisplay.sys	Microsoft Corporation	Microsoft Windows	
BasicRender (BasicRender)	Running/System	C:\Windows\system32\drivers\BasicRender.sys	Microsoft Corporation	Microsoft Windows	
bfadfcoei (bfadfcoei)	Stopped/Manual	C:\Windows\system32\drivers\bfadfcoei.sys	Brocade Communications Systems, Inc.	Microsoft Windows	
bfadi (bfadi)	Stopped/Manual	C:\Windows\system32\drivers\bfadi.sys	Brocade Communications Systems, Inc.	Microsoft Windows	
bowser (Browser Support Driver)	Running/Manual	C:\Windows\system32\drivers\bowser.sys	Microsoft Corporation	Microsoft Windows	
bxfcoe (Broadcom NetXtreme II Offload FCoE Driver)	Stopped/Manual	C:\Windows\system32\drivers\bxfcoe.sys	Broadcom Corporation	Microsoft Windows	
bxois (Broadcom NetXtreme II Offload iSCSI Driver)	Running/Boot	C:\Windows\system32\drivers\bxois.sys	Broadcom Corporation	Broadcom Corporation	
cdfs (CD/DVD File System Reader)	Stopped/Disabled	C:\Windows\system32\drivers\cdfs.sys	Microsoft Corporation	Microsoft Windows	
cdrom (CD-ROM Driver)	Stopped/System	C:\Windows\system32\drivers\cdrom.sys	Microsoft Corporation	Microsoft Windows	
cht4vbd (Chelsio T4 Virtual Bus Driver)	Stopped/Manual	C:\Windows\system32\drivers\cht4vx64.sys	Chelsio Communications	Microsoft Windows	
CLFS (Common Log (CLFS))	Running/Boot	C:\Windows\system32\drivers\clfs.sys	Microsoft Corporation	Microsoft Windows	
CmBatt (Microsoft ACPI Control Method Battery Driver)	Stopped/Manual	C:\Windows\system32\drivers\CmBatt.sys	Microsoft Corporation	Microsoft Windows	

Driver	Status	Exe	Company	Signer	Recommendation
CNG (CNG)	Running/Boot	C:\Windows\system32\drivers\cng.sys	Microsoft Corporation	Microsoft Windows	
CompositeBus (Composite Bus Enumerator Driver)	Running/Manual	C:\Windows\system32\drivers\CompositeBus.sys	Microsoft Corporation	Microsoft Windows	
condrv (Console Driver)	Running/Manual	C:\Windows\system32\drivers\condrv.sys	Microsoft Corporation	Microsoft Windows	
dcdbas (System Management Driver)	Running/Manual	C:\Windows\system32\drivers\dcdbas64.sys	Dell Inc.	Dell Inc.	
Dedup (Dedup)	Running/System	C:\Windows\system32\drivers\dedup.sys	Microsoft Corporation	Microsoft Windows	
Dfsc (DFS Namespace Client Driver)	Running/System	C:\Windows\system32\drivers\dfsc.sys	Microsoft Corporation	Microsoft Windows	
DIRECTIO (DIRECTIO)	Stopped/Manual	(unresolved) \??\E:\Performancetest\DirectIo64.sys	?	<no signature>	☹ check the origin of the driver
disk (Disk Driver)	Running/Boot	C:\Windows\system32\drivers\disk.sys	Microsoft Corporation	Microsoft Windows	
dmvsc (dmvsc)	Stopped/Manual	C:\Windows\system32\drivers\dmvsc.sys	Microsoft Corporation	Microsoft Windows	
DXGKrnl (LDDM Graphics Subsystem)	Running/Manual	C:\Windows\system32\drivers\dxgkrnl.sys	Microsoft Corporation	Microsoft Windows	
ebdrv (Broadcom NetXtreme II 10 GigE VBD)	Stopped/Manual	C:\Windows\system32\drivers\evbda.sys	Broadcom Corporation	Microsoft Windows	
elxfcoe (elxfcoe)	Stopped/Manual	C:\Windows\system32\drivers\elxfcoe.sys	Emulex	Microsoft Windows	
elxstor (elxstor)	Stopped/Manual	C:\Windows\system32\drivers\elxstor.sys	Emulex	Microsoft Windows	
ErrDev (Microsoft Hardware Error Device Driver)	Running/Manual	C:\Windows\system32\drivers\errdev.sys	Microsoft Corporation	Microsoft Windows	
fcvsc (fcvsc)	Stopped/Manual	C:\Windows\system32\drivers\fcvsc.sys	Microsoft Corporation	Microsoft Windows	
fdc (Floppy Disk Controller Driver)	Stopped/Manual	C:\Windows\system32\drivers\fdc.sys	Microsoft Corporation	Microsoft Windows	
FileInfo (File Information FS MiniFilter)	Stopped/Manual	C:\Windows\system32\drivers\fileinfo.sys	Microsoft Corporation	Microsoft Windows	
Filetrace (Filetrace)	Stopped/Manual	C:\Windows\system32\drivers\filetrace.sys	Microsoft Corporation	Microsoft Windows	
flpydisk (Floppy Disk Driver)	Stopped/Manual	C:\Windows\system32\drivers\flpydisk.sys	Microsoft Corporation	Microsoft Windows	
FltMgr (FltMgr)	Running/Boot	C:\Windows\system32\drivers\fltMgr.sys	Microsoft Corporation	Microsoft Windows	
FsDepends (File System Dependency Minifilter)	Stopped/Manual	C:\Windows\system32\drivers\FsDepends.sys	Microsoft Corporation	Microsoft Windows	
FxPPM (Power Framework Processor Driver)	Stopped/Manual	C:\Windows\system32\drivers\fxppm.sys	Microsoft Corporation	Microsoft Windows	
gagp30kx (Microsoft Generic AGPv3.0 Filter for K8 Processor Platforms)	Stopped/Manual	C:\Windows\system32\drivers\GAGP30KX.SYS	Microsoft Corporation	Microsoft Windows	
gencounter (Microsoft Hyper-V Generation Counter)	Stopped/Manual	C:\Windows\system32\drivers\vmgencounter.sys	Microsoft Corporation	Microsoft Windows	
GPIOClx0101 (Microsoft GPIO Class Extension Driver)	Stopped/Manual	C:\Windows\system32\drivers\msgpioclx.sys	Microsoft Corporation	Microsoft Windows	
HDAudBus (Microsoft UAA Bus Driver for High Definition Audio)	Stopped/Manual	C:\Windows\system32\drivers\hdaudbus.sys	Microsoft Corporation	Microsoft Windows	

Driver	Status	Exe	Company	Signer	Recommendation
HidBatt (HID UPS Battery Driver)	Stopped/Manual	C:\Windows\system32\drivers\hidbatt.sys	Microsoft Corporation	Microsoft Windows	
HidUsb (Microsoft HID Class Driver)	Running/Manual	C:\Windows\system32\drivers\hidusb.sys	Microsoft Corporation	Microsoft Windows	
HpSAMD (HpSAMD)	Stopped/Manual	C:\Windows\system32\drivers\HpSAMD.sys	Hewlett-Packard Company	Microsoft Windows	
HTTP (HTTP Service)	Running/Manual	C:\Windows\system32\drivers\http.sys	Microsoft Corporation	Microsoft Windows	
hwpolicy (Hardware Policy Driver)	Stopped/Boot	C:\Windows\system32\drivers\hwpolicy.sys	Microsoft Corporation	Microsoft Windows	
hyperkbd (hyperkbd)	Stopped/Manual	C:\Windows\system32\drivers\hyperkbd.sys	Microsoft Corporation	Microsoft Windows	
HyperVideo (HyperVideo)	Stopped/Manual	C:\Windows\system32\drivers\HyperVideo.sys	Microsoft Corporation	Microsoft Windows	
i8042prt (PS/2 Keyboard and Mouse Port Driver)	Stopped/Manual	C:\Windows\system32\drivers\i8042prt.sys	Microsoft Corporation	Microsoft Windows	
iaStorAV (Intel(R) SATA RAID Controller Windows)	Stopped/Manual	C:\Windows\system32\drivers\iaStorAV.sys	Intel Corporation	Microsoft Windows	
iaStorV (Intel RAID Controller Windows 7)	Stopped/Manual	C:\Windows\system32\drivers\iaStorV.sys	Intel Corporation	Microsoft Windows	
ibbus (Mellanox InfiniBand Bus/AL (Filter Driver))	Stopped/Manual	C:\Windows\system32\drivers\ibbus.sys	Mellanox	Microsoft Windows	
intelide (intelide)	Stopped/Manual	C:\Windows\system32\drivers\intelide.sys	Microsoft Corporation	Microsoft Windows	
intelppm (Intel Processor Driver)	Stopped/Manual	C:\Windows\system32\drivers\intelppm.sys	Microsoft Corporation	Microsoft Windows	
IpFilterDriver (IP Traffic Filter Driver)	Stopped/Manual	C:\Windows\system32\drivers\ipfltdrv.sys	Microsoft Corporation	Microsoft Windows	
IPMIDRV (IPMIDRV)	Running/Manual	C:\Windows\system32\drivers\IPMIDrv.sys	Microsoft Corporation	Microsoft Windows	
IPNAT (IP Network Address Translator)	Stopped/Manual	C:\Windows\system32\drivers\ipnat.sys	Microsoft Corporation	Microsoft Windows	
isapnp (isapnp)	Stopped/Manual	C:\Windows\system32\drivers\isapnp.sys	Microsoft Corporation	Microsoft Windows	
iScsiPrt (iScsiPort Driver)	Stopped/Manual	C:\Windows\system32\drivers\msiscsi.sys	Microsoft Corporation	Microsoft Windows	
kbdclass (Keyboard Class Driver)	Running/Manual	C:\Windows\system32\drivers\kbdclass.sys	Microsoft Corporation	Microsoft Windows	
kbdhid (Keyboard HID Driver)	Running/Manual	C:\Windows\system32\drivers\kbdhid.sys	Microsoft Corporation	Microsoft Windows	
kdnic (Microsoft Kernel Debug Network Miniport (NDIS 6.20))	Running/Manual	C:\Windows\system32\drivers\kdnic.sys	Microsoft Corporation	Microsoft Windows	
KSecDD (KSecDD)	Running/Boot	C:\Windows\system32\drivers\ksecdd.sys	Microsoft Corporation	Microsoft Windows	
KSecPkg (KSecPkg)	Running/Boot	C:\Windows\system32\drivers\ksecpkg.sys	Microsoft Corporation	Microsoft Windows	
ksthunk (Kernel Streaming Thunks)	Stopped/Manual	C:\Windows\system32\drivers\ksthunk.sys	Microsoft Corporation	Microsoft Windows	
l2nd (Broadcom NetXtreme II BXND)	Running/Manual	C:\Windows\system32\drivers\bxnd60a.sys	Broadcom Corporation	Broadcom Corporation	
lltdio (Link-Layer Topology Discovery Mapper I/O Driver)	Running/Auto	C:\Windows\system32\drivers\lltdio.sys	Microsoft Corporation	Microsoft Windows	
LSI_SAS (LSI_SAS)	Stopped/Manual	C:\Windows\system32\drivers\lsi_sas.sys	LSI Corporation	Microsoft Windows	
LSI_SAS2 (LSI_SAS2)	Stopped/Manual	C:\Windows\system32\drivers\lsi_sas2.sys	LSI Corporation	Microsoft Windows	

Driver	Status	Exe	Company	Signer	Recommendation
LSI_SAS3 (LSI_SAS3)	Stopped/Manual	C:\Windows\system32\drivers\lsi_sas3.sys	LSI Corporation	Microsoft Windows	
LSI_SSS (LSI_SSS)	Stopped/Manual	C:\Windows\system32\drivers\lsi_sss.sys	LSI Corporation	Microsoft Windows	
luafv (UAC File Virtualization)	Running/Auto	C:\Windows\system32\drivers\luafv.sys	Microsoft Corporation	Microsoft Windows	
megasas (megasas)	Running/Boot	C:\Windows\system32\drivers\megasas.sys	LSI Corporation	Microsoft Windows	
megasr (megasr)	Stopped/Manual	C:\Windows\system32\drivers\megasr.sys	LSI Corporation, Inc.	Microsoft Windows	
mlx4_bus (Mellanox ConnectX Bus Enumerator)	Stopped/Manual	C:\Windows\system32\drivers\mlx4_bus.sys	Mellanox	Microsoft Windows	
Modem (Modem)	Stopped/Manual	C:\Windows\system32\drivers\modem.sys	Microsoft Corporation	Microsoft Windows	
monitor (Microsoft Monitor Class Function Driver Service)	Running/Manual	C:\Windows\system32\drivers\monitor.sys	Microsoft Corporation	Microsoft Windows	
mouclass (Mouse Class Driver)	Running/Manual	C:\Windows\system32\drivers\mouclass.sys	Microsoft Corporation	Microsoft Windows	
mouhid (Mouse HID Driver)	Running/Manual	C:\Windows\system32\drivers\mouhid.sys	Microsoft Corporation	Microsoft Windows	
mountmgr (Mount Point Manager)	Running/Boot	C:\Windows\system32\drivers\mountmgr.sys	Microsoft Corporation	Microsoft Windows	
mpsdrv (Windows Firewall Authorization Driver)	Running/Manual	C:\Windows\system32\drivers\mpsdrv.sys	Microsoft Corporation	Microsoft Windows	
mrxsmb (SMB MiniRedirector Wrapper and Engine)	Running/Manual	C:\Windows\system32\drivers\mrxsmb.sys	Microsoft Corporation	Microsoft Windows	
mrxsmb10 (SMB 1.x MiniRedirector)	Running/Auto	C:\Windows\system32\drivers\mrxsmb10.sys	Microsoft Corporation	Microsoft Windows	
mrxsmb20 (SMB 2.0 MiniRedirector)	Running/Manual	C:\Windows\system32\drivers\mrxsmb20.sys	Microsoft Corporation	Microsoft Windows	
MsBridge (Microsoft MAC Bridge)	Stopped/Manual	C:\Windows\system32\drivers\bridge.sys	Microsoft Corporation	Microsoft Windows	
mshidkmdf (Pass-through HID to KMDF Filter Driver)	Stopped/Manual	C:\Windows\system32\drivers\mshidkmdf.sys	Microsoft Corporation	Microsoft Windows	
mshidumdf (Pass-through HID to UMDF Driver)	Stopped/Manual	C:\Windows\system32\drivers\mshidumdf.sys	Microsoft Corporation	Microsoft Windows	
msisadrv (msisadrv)	Running/Boot	C:\Windows\system32\drivers\msisadrv.sys	Microsoft Corporation	Microsoft Windows	
MsLbfoProvider (Microsoft Load Balancing/Failover Provider)	Running/Auto	C:\Windows\system32\drivers\MsLbfoProvider.sys	Microsoft Corporation	Microsoft Windows	
mssmbios (Microsoft System Management BIOS Driver)	Running/System	C:\Windows\system32\drivers\mssmbios.sys	Microsoft Corporation	Microsoft Windows	
MTConfig (Microsoft Input Configuration Driver)	Stopped/Manual	C:\Windows\system32\drivers\MTConfig.sys	Microsoft Corporation	Microsoft Windows	
Mup (Mup)	Running/Boot	C:\Windows\system32\drivers\mup.sys	Microsoft Corporation	Microsoft Windows	
mvumis (mvumis)	Stopped/Manual	C:\Windows\system32\drivers\mvumis.sys	Marvell Semiconductor, Inc.	Microsoft Windows	
MxG2wDO64 (MxG2wDO64)	Running/Manual	C:\Windows\system32\drivers\MxG2wDO64	Matrox Graphics Inc.	Microsoft Windows Hardware	

Driver	Status	Exe	Company	Signer	Recommendation
		.sys		Compatibility Publisher	
ndfltr (NetworkDirect Service)	Stopped/Manual	C:\Windows\system32\drivers\ndfltr.sys	Mellanox	Microsoft Windows	
NDIS (NDIS System Driver)	Running/Boot	C:\Windows\system32\drivers\ndis.sys	Microsoft Corporation	Microsoft Windows	
NdisCap (Microsoft NDIS Capture)	Stopped/Manual	C:\Windows\system32\drivers\ndiscap.sys	Microsoft Corporation	Microsoft Windows	
NdisImPlatform (Microsoft Network Adapter Multiplexor Protocol)	Stopped/Manual	C:\Windows\system32\drivers\NdisImPlatform.sys	Microsoft Corporation	Microsoft Windows	
NdisImPlatformMp (Microsoft Network Adapter Multiplexor Driver)	Running/Manual	C:\Windows\system32\drivers\NdisImPlatform.sys	Microsoft Corporation	Microsoft Windows	
NdisTapi (Remote Access NDIS TAPI Driver)	Running/Manual	C:\Windows\system32\drivers\ndistapi.sys	Microsoft Corporation	Microsoft Windows	
Ndisuio (NDIS Usermode I/O Protocol)	Stopped/Manual	C:\Windows\system32\drivers\ndisuio.sys	Microsoft Corporation	Microsoft Windows	
NdisVirtualBus (Microsoft Virtual Network Adapter Enumerator)	Running/Manual	C:\Windows\system32\drivers\NdisVirtualBus.sys	Microsoft Corporation	Microsoft Windows	
NdisWan (Remote Access NDIS WAN Driver)	Running/Manual	C:\Windows\system32\drivers\ndiswan.sys	Microsoft Corporation	Microsoft Windows	
NDISWANLEGACY (Remote Access LEGACY NDIS WAN Driver)	Stopped/Manual	C:\Windows\system32\drivers\ndiswan.sys	Microsoft Corporation	Microsoft Windows	
NetBIOS (NetBIOS Interface)	Running/System	C:\Windows\system32\drivers\netbios.sys	Microsoft Corporation	Microsoft Windows	
NetBT (NetBT)	Running/System	C:\Windows\system32\drivers\netbt.sys	Microsoft Corporation	Microsoft Windows	
netvsc (netvsc)	Stopped/Manual	C:\Windows\system32\drivers\netvsc63.sys	Microsoft Corporation	Microsoft Windows	
NPF (NetGroup Packet Filter Driver)	Running/Auto	C:\Windows\system32\drivers\npf.sys	Riverbed Technology, Inc.	Riverbed Technology, Inc.	
npsvctrig (Named pipe service trigger provider)	Running/System	C:\Windows\system32\drivers\npsvctrig.sys	Microsoft Corporation	Microsoft Windows	
nsiproxy (NSI Proxy Service Driver)	Running/System	C:\Windows\system32\drivers\nsiproxy.sys	Microsoft Corporation	Microsoft Windows	
nv_agp (NVIDIA nForce AGP Bus Filter)	Stopped/Manual	C:\Windows\system32\drivers\NV_AGP.SYS	Microsoft Corporation	Microsoft Windows	
nvraid (nvraid)	Stopped/Manual	C:\Windows\system32\drivers\nvraid.sys	NVIDIA Corporation	Microsoft Windows	
nvstor (nvstor)	Stopped/Manual	C:\Windows\system32\drivers\nvstor.sys	NVIDIA Corporation	Microsoft Windows	
Parport (Parallel port driver)	Stopped/Manual	C:\Windows\system32\drivers\parport.sys	Microsoft Corporation	Microsoft Windows	
partmgr (Partition Manager)	Running/Boot	C:\Windows\system32\drivers\partmgr.sys	Microsoft Corporation	Microsoft Windows	
pci (PCI Bus Driver)	Running/Boot	C:\Windows\system32\drivers\pci.sys	Microsoft Corporation	Microsoft Windows	
pciide (pciide)	Stopped/Manual	C:\Windows\system32\drivers\pciide.sys	Microsoft Corporation	Microsoft Windows	
pcmcia (pcmcia)	Stopped/Manual	C:\Windows\system32\drivers\pcmcia.sys	Microsoft Corporation	Microsoft Windows	
pcw (Performance Counters for Windows	Running/Boot	C:\Windows\system32\drivers\pcw.sys	Microsoft Corporation	Microsoft Windows	

Driver	Status	Exe	Company	Signer	Recommendation
Driver)					
pdc (pdc)	Running/Boot	C:\Windows\system32\drivers\pdc.sys	Microsoft Corporation	Microsoft Windows	
PEAUTH (PEAUTH)	Running/Auto	C:\Windows\system32\drivers\PEAuth.sys	Microsoft Corporation	Microsoft Windows	
PptpMiniport (WAN Miniport (PPTP))	Running/Manual	C:\Windows\system32\drivers\raspptp.sys	Microsoft Corporation	Microsoft Windows	
Processor (Processor Driver)	Stopped/Manual	C:\Windows\system32\drivers\processr.sys	Microsoft Corporation	Microsoft Windows	
Psched (QoS Packet Scheduler)	Running/System	C:\Windows\system32\drivers\pacer.sys	Microsoft Corporation	Microsoft Windows	
ql2300i (QLogic Fibre Channel STOR Miniport Inbox Driver (wx64))	Stopped/Manual	C:\Windows\system32\drivers\ql2300i.sys	QLogic Corporation	Microsoft Windows	
ql40xx2i (QLogic iSCSI Miniport Inbox Driver)	Stopped/Manual	C:\Windows\system32\drivers\ql40xx2i.sys	QLogic Corporation	Microsoft Windows	
qlfcoei (QLogic [FCoE] STOR Miniport Inbox Driver (wx64))	Stopped/Manual	C:\Windows\system32\drivers\qlfcoei.sys	QLogic Corporation	Microsoft Windows	
RasAcd (Remote Access Auto Connection Driver)	Stopped/Manual	C:\Windows\system32\drivers\rasacd.sys	Microsoft Corporation	Microsoft Windows	
RasAgileVpn (WAN Miniport (IKEv2))	Running/Manual	C:\Windows\system32\drivers\agilevpn.sys	Microsoft Corporation	Microsoft Windows	
Rasl2tp (WAN Miniport (L2TP))	Running/Manual	C:\Windows\system32\drivers\rasl2tp.sys	Microsoft Corporation	Microsoft Windows	
RasPppoe (Remote Access PPPOE Driver)	Running/Manual	C:\Windows\system32\drivers\raspppoe.sys	Microsoft Corporation	Microsoft Windows	
RasSstp (WAN Miniport (SSTP))	Running/Manual	C:\Windows\system32\drivers\rassstp.sys	Microsoft Corporation	Microsoft Windows	
rdbss (Redirected Buffering Sub System)	Running/System	C:\Windows\system32\drivers\rdbss.sys	Microsoft Corporation	Microsoft Windows	
rdpbus (Remote Desktop Device Redirector Bus Driver)	Running/Manual	C:\Windows\system32\drivers\rdpbus.sys	Microsoft Corporation	Microsoft Windows	
RDPDR (Remote Desktop Device Redirector Driver)	Running/Manual	C:\Windows\system32\drivers\rdpdr.sys	Microsoft Corporation	Microsoft Windows	
RdpVideoMiniport (Remote Desktop Video Miniport Driver)	Running/Manual	C:\Windows\system32\drivers\rdpvideominiport.sys	Microsoft Corporation	Microsoft Windows	
RsFx0151 (RsFx0151 Driver)	Stopped/Disabled	C:\Windows\system32\drivers\RsFx0151.sys	Microsoft Corporation	Microsoft Corporation	
RsFx0201 (RsFx0201 Driver)	Stopped/Disabled	C:\Windows\system32\drivers\RsFx0201.sys	Microsoft Corporation	Microsoft Corporation	
rspndr (Link-Layer Topology Discovery Responder)	Running/Auto	C:\Windows\system32\drivers\rspndr.sys	Microsoft Corporation	Microsoft Windows	
s3cap (s3cap)	Stopped/Manual	C:\Windows\system32\drivers\vms3cap.sys	Microsoft Corporation	Microsoft Windows	
sacdrv (sacdrv)	Stopped/Boot	C:\Windows\system32\drivers\sacdrv.sys	Microsoft Corporation	Microsoft Windows	
sbp2port (SBP-2 Transport/Protocol Bus Driver)	Stopped/Manual	C:\Windows\system32\drivers\sbp2port.sys	Microsoft Corporation	Microsoft Windows	
scfilter (Smart card PnP Class Filter Driver)	Stopped/Manual	C:\Windows\system32\drivers\scfilter.sys	Microsoft Corporation	Microsoft Windows	
sdbus (sdbus)	Stopped/Manual	C:\Windows\system32\drivers\sdbus.sys	Microsoft Corporation	Microsoft Windows	
sdstor (SD Storage	Stopped/Manual	C:\Windows\system32	Microsoft Corporation	Microsoft Windows	

Driver	Status	Exe	Company	Signer	Recommendation
Port Driver)		\drivers\sdstor.sys			
SerCx (Serial UART Support Library)	Stopped/Manual	C:\Windows\system32 \drivers\SerCx.sys	Microsoft Corporation	Microsoft Windows	
SerCx2 (Serial UART Support Library)	Stopped/Manual	C:\Windows\system32 \drivers\SerCx2.sys	Microsoft Corporation	Microsoft Windows	
Serenum (Serenum Filter Driver)	Running/Manual	C:\Windows\system32 \drivers\serenum.sys	Microsoft Corporation	Microsoft Windows	
Serial (Serial port driver)	Running/Manual	C:\Windows\system32 \drivers\serial.sys	Microsoft Corporation	Microsoft Windows	
sermouse (Serial Mouse Driver)	Stopped/Manual	C:\Windows\system32 \drivers\sermouse.sys	Microsoft Corporation	Microsoft Windows	
sfloppy (High-Capacity Floppy Disk Drive)	Stopped/Manual	C:\Windows\system32 \drivers\sfloppy.sys	Microsoft Corporation	Microsoft Windows	
SiSRaid2 (SiSRaid2)	Stopped/Manual	C:\Windows\system32 \drivers\sisraid2.sys	Silicon Integrated Systems Corp.	Microsoft Windows	
SiSRaid4 (SiSRaid4)	Stopped/Manual	C:\Windows\system32 \drivers\sisraid4.sys	Silicon Integrated Systems	Microsoft Windows	
smbdirect (smbdirect)	Stopped/Manual	C:\Windows\system32 \drivers\smbdirect.sys	Microsoft Corporation	Microsoft Windows	
spaceport (Storage Spaces Driver)	Running/Boot	C:\Windows\system32 \drivers\spaceport.sys	Microsoft Corporation	Microsoft Windows	
SpbCx (Simple Peripheral Bus Support Library)	Stopped/Manual	C:\Windows\system32 \drivers\SpbCx.sys	Microsoft Corporation	Microsoft Windows	
srv (Server SMB 1.xxx Driver)	Running/Auto	C:\Windows\system32 \drivers\srv.sys	Microsoft Corporation	Microsoft Windows	
srv2 (Server SMB 2.xxx Driver)	Running/Manual	C:\Windows\system32 \drivers\srv2.sys	Microsoft Corporation	Microsoft Windows	
srvnet (srvnet)	Running/Manual	C:\Windows\system32 \drivers\srvnet.sys	Microsoft Corporation	Microsoft Windows	
stexstor (stexstor)	Stopped/Manual	C:\Windows\system32 \drivers\stexstor.sys	Promise Technology, Inc.	Microsoft Windows	
storahci (Microsoft Standard SATA AHCI Driver)	Stopped/Manual	C:\Windows\system32 \drivers\storahci.sys	Microsoft Corporation	Microsoft Windows	
storflt (Hyper-V Storage Accelerator)	Stopped/Manual	C:\Windows\system32 \drivers\vmstorfl.sys	Microsoft Corporation	Microsoft Windows	
stornvme (Microsoft Standard NVM Express Driver)	Stopped/Manual	C:\Windows\system32 \drivers\stornvme.sys	Microsoft Corporation	Microsoft Windows	
storvsc (storvsc)	Stopped/Manual	C:\Windows\system32 \drivers\storvsc.sys	Microsoft Corporation	Microsoft Windows	
storvsp (storvsp)	Stopped/Manual	C:\Windows\system32 \drivers\storvsp.sys	Microsoft Corporation	Microsoft Windows	
swenum (Software Bus Driver)	Running/Manual	C:\Windows\system32 \drivers\swenum.sys	Microsoft Corporation	Microsoft Windows	
Tcpip (TCP/IP Protocol Driver)	Running/Boot	C:\Windows\system32 \drivers\tcpip.sys	Microsoft Corporation	Microsoft Windows	
TCPIP6 (Microsoft IPv6 Protocol Driver)	Stopped/Manual	C:\Windows\system32 \drivers\tcpip.sys	Microsoft Corporation	Microsoft Windows	
tcpipreg (TCP/IP Registry Compatibility)	Running/Auto	C:\Windows\system32 \drivers\tcpipreg.sys	Microsoft Corporation	Microsoft Windows	
tdx (NetIO Legacy TDI Support Driver)	Running/System	C:\Windows\system32 \drivers\tdx.sys	Microsoft Corporation	Microsoft Windows	
terminpt (Microsoft Remote Desktop Input Driver)	Running/Manual	C:\Windows\system32 \drivers\terminpt.sys	Microsoft Corporation	Microsoft Windows	
TPM (TPM)	Running/Manual	C:\Windows\system32 \drivers\tpm.sys	Microsoft Corporation	Microsoft Windows	
TsUsbFlt (TsUsbFlt)	Stopped/Manual	C:\Windows\system32 \drivers\TsUsbFlt.sys	Microsoft Corporation	Microsoft Windows	
TsUsbGD (Remote Desktop Generic USB	Stopped/Manual	C:\Windows\system32 \drivers\TsUsbGD.sys	Microsoft Corporation	Microsoft Windows	

Driver	Status	Exe	Company	Signer	Recommendation
Device)					
tsusbhub (Remote Desktop USB Hub)	Stopped/Manual	C:\Windows\system32\drivers\tsusbhub.sys	Microsoft Corporation	Microsoft Windows	
tunnel (Microsoft Tunnel Miniport Adapter Driver)	Running/Manual	C:\Windows\system32\drivers\tunnel.sys	Microsoft Corporation	Microsoft Windows	
uagp35 (Microsoft AGPv3.5 Filter)	Stopped/Manual	C:\Windows\system32\drivers\UAGP35.SYS	Microsoft Corporation	Microsoft Windows	
UASPStor (USB Attached SCSI (UAS) Driver)	Stopped/Manual	C:\Windows\system32\drivers\uaspstor.sys	Microsoft Corporation	Microsoft Windows	
UCX01000 (USB Controller Extension)	Stopped/Manual	C:\Windows\system32\drivers\UCX01000.SYS	Microsoft Corporation	Microsoft Windows	
udfs (udfs)	Stopped/Disabled	C:\Windows\system32\drivers\udfs.sys	Microsoft Corporation	Microsoft Windows	
UEFI (Microsoft UEFI Driver)	Stopped/Manual	C:\Windows\system32\drivers\uefi.sys	Microsoft Corporation	Microsoft Windows	
uliagpkx (Uli AGP Bus Filter)	Stopped/Manual	C:\Windows\system32\drivers\ULIAGPKX.SYS	Microsoft Corporation	Microsoft Windows	
umbus (UMBus Enumerator Driver)	Running/Manual	C:\Windows\system32\drivers\umbus.sys	Microsoft Corporation	Microsoft Windows	
UmPass (Microsoft UMPass Driver)	Stopped/Manual	C:\Windows\system32\drivers\umpass.sys	Microsoft Corporation	Microsoft Windows	
usbccgp (Microsoft USB Generic Parent Driver)	Running/Manual	C:\Windows\system32\drivers\usbccgp.sys	Microsoft Corporation	Microsoft Windows	
usbehci (Microsoft USB 2.0 Enhanced Host Controller Miniport Driver)	Running/Manual	C:\Windows\system32\drivers\usbehci.sys	Microsoft Corporation	Microsoft Windows	
usbhub (Microsoft USB Standard Hub Driver)	Running/Manual	C:\Windows\system32\drivers\usbhub.sys	Microsoft Corporation	Microsoft Windows	
USBHUB3 (SuperSpeed Hub)	Stopped/Manual	C:\Windows\system32\drivers\USBHUB3.SYS	Microsoft Corporation	Microsoft Windows	
usbohci (Microsoft USB Open Host Controller Miniport Driver)	Running/Manual	C:\Windows\system32\drivers\usbohci.sys	Microsoft Corporation	Microsoft Windows	
usbprint (Microsoft USB PRINTER Class)	Stopped/Manual	C:\Windows\system32\drivers\usbprint.sys	Microsoft Corporation	Microsoft Windows	
USBSTOR (USB Mass Storage Driver)	Stopped/Manual	C:\Windows\system32\drivers\USBSTOR.SYS	Microsoft Corporation	Microsoft Windows	
usbuhci (Microsoft USB Universal Host Controller Miniport Driver)	Stopped/Manual	C:\Windows\system32\drivers\usbuhci.sys	Microsoft Corporation	Microsoft Windows	
USBXHCI (USB xHCI Compliant Host Controller)	Stopped/Manual	C:\Windows\system32\drivers\USBXHCI.SYS	Microsoft Corporation	Microsoft Windows	
vdrvroot (Microsoft Virtual Drive Enumerator)	Running/Boot	C:\Windows\system32\drivers\vdrvroot.sys	Microsoft Corporation	Microsoft Windows	
VeeamFSR (VeeamFSR)	Running/Auto	C:\Program Files (x86)\Veeam\Backup Transport\VeeamFSR.sys	Veeam Software AG	Veeam Software AG	☹ quote ImagePath
VerifierExt (VerifierExt)	Stopped/Manual	C:\Windows\system32\drivers\VerifierExt.sys	Microsoft Corporation	Microsoft Windows	

Driver	Status	Exe	Company	Signer	Recommendation
vhdmp (vhdmp)	Stopped/Manual	C:\Windows\system32\drivers\vhdmp.sys	Microsoft Corporation	Microsoft Windows	
viaide (viaide)	Stopped/Manual	C:\Windows\system32\drivers\viaide.sys	VIA Technologies, Inc.	Microsoft Windows	
Vid (Vid)	Stopped/Manual	C:\Windows\system32\drivers\Vid.sys	Microsoft Corporation	Microsoft Windows	
VirtualDK (VirtualDK)	Stopped/Manual	C:\Program Files\Veeam\Backup and Replication\Backup\vdk.sys	Ken Kato	Veeam Software AG	☹ quote ImagePath
vmbus (Virtual Machine Bus)	Stopped/Manual	C:\Windows\system32\drivers\vmbus.sys	Microsoft Corporation	Microsoft Windows	
VMBusHID (VMBusHID)	Stopped/Manual	C:\Windows\system32\drivers\VMBusHID.sys	Microsoft Corporation	Microsoft Windows	
vmbusr (Virtual Machine Bus Provider)	Stopped/Manual	C:\Windows\system32\drivers\vmbusr.sys	Microsoft Corporation	Microsoft Windows	
volmgr (Volume Manager Driver)	Running/Boot	C:\Windows\system32\drivers\volmgr.sys	Microsoft Corporation	Microsoft Windows	
volmgrx (Dynamic Volume Manager)	Running/Boot	C:\Windows\system32\drivers\volmgrx.sys	Microsoft Corporation	Microsoft Windows	
volsnap (Storage volumes)	Running/Boot	C:\Windows\system32\drivers\volsnap.sys	Microsoft Corporation	Microsoft Windows	
vpci (Microsoft Hyper-V Virtual PCI Bus)	Stopped/Manual	C:\Windows\system32\drivers\vpci.sys	Microsoft Corporation	Microsoft Windows	
vpcivsp (Microsoft Hyper-V PCI Server)	Stopped/Manual	C:\Windows\system32\drivers\vpcivsp.sys	Microsoft Corporation	Microsoft Windows	
vsmraid (vsmraid)	Stopped/Manual	C:\Windows\system32\drivers\vsmraid.sys	VIA Technologies Inc.,Ltd	Microsoft Windows	
VSTXRAID (VIA StorX Storage RAID Controller Windows Driver)	Stopped/Manual	C:\Windows\system32\drivers\VSTXRAID.SYS	VIA Corporation	Microsoft Windows	
WacomPen (Wacom Serial Pen HID Driver)	Stopped/Manual	C:\Windows\system32\drivers\wacompen.sys	Microsoft Corporation	Microsoft Windows	
Wanarp (Remote Access IP ARP Driver)	Stopped/Manual	C:\Windows\system32\drivers\wanarp.sys	Microsoft Corporation	Microsoft Windows	
Wanarpv6 (Remote Access IPv6 ARP Driver)	Running/System	C:\Windows\system32\drivers\wanarp.sys	Microsoft Corporation	Microsoft Windows	
Wdf01000 (Kernel Mode Driver Frameworks service)	Running/Boot	C:\Windows\system32\drivers\Wdf01000.sys	Microsoft Corporation	Microsoft Windows	
WFPLWFS (Microsoft Windows Filtering Platform)	Running/Boot	C:\Windows\system32\drivers\wfplwfs.sys	Microsoft Corporation	Microsoft Windows	
WIMMount (WIMMount)	Stopped/Manual	C:\Windows\system32\drivers\wimmount.sys	Microsoft Corporation	Microsoft Windows	
WinMad (WinMad Service)	Stopped/Manual	C:\Windows\system32\drivers\winmad.sys	Mellanox	Microsoft Windows	
WinNat (Windows NAT Driver)	Stopped/Manual	C:\Windows\system32\drivers\winnat.sys	Microsoft Corporation	Microsoft Windows	
WinVerbs (WinVerbs Service)	Stopped/Manual	C:\Windows\system32\drivers\winverbs.sys	Mellanox	Microsoft Windows	
WmiAcpi (Microsoft Windows Management Interface for ACPI)	Stopped/Manual	C:\Windows\system32\drivers\wmiacpi.sys	Microsoft Corporation	Microsoft Windows	
ws2ifsl (Winsock IFS Driver)	Stopped/Disabled	C:\Windows\system32\drivers\ws2ifsl.sys	Microsoft Corporation	Microsoft Windows	
wtlmdrv (Microsoft iSCSI Target	Stopped/Manual	C:\Windows\system32\drivers\wtlmdrv.sys	Microsoft Corporation	Microsoft Windows	

Driver	Status	Exe	Company	Signer	Recommendation
LocalMount Adapter)					
WudfPf (User Mode Driver Frameworks Platform Driver)	Stopped/Manual	C:\Windows\system32\drivers\WUDFPf.sys	Microsoft Corporation	Microsoft Windows	

[Computer ERZA] [Top][Summary][Explanatory notes]

1.3.3 [SVCS-03] Services and drivers access permissions

The check verifies access permissions (ACLs) of system services and drivers. The check fails if there is a service with non-std. owner, or there is a service whose configuration can be modified by non-privileged users, or there is a service which can be started/stopped by an anonymous user. Exceptions can be defined by check parameters if necessary. Services which fail to satisfy the above rules are shown in the results table together with detailed specifications of the problem.

Check result: OK.

[Computer ERZA] [Top][Summary][Explanatory notes]

1.3.4 [SVCS-04] Service accounts

The check verifies privilege level of accounts, which are used to run system services. If the account of any service falls into one of the privilege levels defined by the check parameters, the overall result of the check is **FAIL**. Exceptions can be defined by other parameters if necessary. Results table lists the problematic services, the account under which they are executed and its privilege level.

Check result: OK.

[Computer ERZA] [Top][Summary][Explanatory notes]

1.3.5 [SVCS-05] Other programs that run automatically

The check verifies access permissions for programs that are just running, that are runnable via PATH environment variable, or that are executed automatically, without direct user action. The permissions must not allow program to be modified by unprivileged users for a successful test result. Exceptions can be specified by check parameters if necessary.

Check result: OK.

[Computer ERZA] [Top][Summary][Explanatory notes]

1.4 [SECP-xx] Security policy

1.4.1 [SECP-01] Passwords and account locking policy

Check verifies the given passwords and accounts locking parameters. Parameters not listed in the profile are not checked.

Check result: FAIL.

We recommend to use the Group Policy to modify these settings. Domain-wide policy object (typically the Default Domain Policy) has to be modified to change the domain accounts policy; for the member servers and workstations local accounts, the policy objects linked to subordinate OU levels can be used as well. GPO settings path is *Computer Configuration(/Policies)/Windows Settings/Security Settings/Account Policies* (and further either *Password Policy* or *Account Lockout Policy* depending on the particular setting).

The values to be verified are listed in the table below. Problematic values are marked in red:

Parameter name	Value	Recommendation
Min password length	10	
Max password age (d)	(no limit)	max. 180
Min password age (d)	0	min. 1
Password history length	0	min. 5
Store passwords using reversible encryption	0	
Password must meet complexity requirements	1	
Account lockout duration (min)	30	
Reset account lockout counter after (min)	30	

Parameter name	Value	Recommendation
Account lockout threshold	10	

[Computer ERZA] [Top][Summary][Explanatory notes]

1.4.2 [SECP-02] Security settings

Check verifies the current settings of the specified system security options.

Check result: FAIL.

Using the Group Policy is recommended to modify these settings. The GPO settings path is *Computer Configuration(/Policies)/Windows Settings/Security Settings/Local Policies/Security Options*.

Note: We strongly recommend thorough testing of the new settings before changing the values in production environment, especially in the case of the parameters affecting network traffic. Potentially the most problematic settings are indicated in table by "[!]".

Security options being verified are listed in the table below. Problematic values are marked in red:

Category	Parameter name	Value	Recommendation
Accounts	Block Microsoft accounts		users can't add or log on with microsoft accounts
	Guest account status	Disabled	
	Limit local account use of blank passwords to console logon only	Enabled	
Devices	Prevent users from installing printer drivers	Enabled	
Domain member	Digitally encrypt or sign secure channel data (always)	Enabled	
	Digitally encrypt secure channel data (when possible)	Enabled	
	Digitally sign secure channel data (when possible)	Enabled	
	Require strong (Windows 2000 or later) session key	Enabled	
Interactive logon	Do not require CTRL+ALT+DEL	Disabled	
	Machine inactivity limit		5-15 min
	Number of previous logons to cache (in case domain controller is not available)	10	0 or 1
Microsoft network client	Digitally sign communications (if server agrees)	Enabled	
	Send unencrypted password to third-party SMB servers	Disabled	
Microsoft network server	Digitally sign communications (if client agrees)	Enabled	
Network access	Allow anonymous SID/Name translation	Disabled	
	Do not allow anonymous enumeration of SAM accounts	Enabled	
	Do not allow anonymous enumeration of SAM accounts and shares	Disabled	enabled [!]
	Do not allow storage of passwords and credentials for network authentication	Disabled	enabled [!]
	Let Everyone permissions apply to anonymous users	Disabled	
	Restrict anonymous access to Named Pipes and Shares	Enabled	
	Sharing and security model for local accounts	Classic: Local users authenticate as themselves	
Network security	Do not store LAN Manager hash value on next password change	Enabled	
	LAN Manager authentication level	Send NTLMv2 response only -	

Category	Parameter name	Value	Recommendation
		refuse LM	
Shutdown	Allow system to be shut down without having to log on	Enabled	☹ disabled
System objects	Require case insensitivity for non-Windows subsystems	Enabled	
	Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled	
User Account Control	Admin Approval Mode for the Built-in Administrator account	Disabled	☹ enabled
	Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled	
	Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent for non-Windows binaries	prompt for consent/credentials on the secure desktop
	Only elevate executables that are signed and validated	Disabled	
	Only elevate UIAccess applications that are installed in secure locations	Enabled	
	Run all administrators in Admin Approval Mode	Enabled	
	Switch to the secure desktop when prompting for elevation	Enabled	
	Virtualize file and registry write failures to per-user locations	Enabled	

[Computer ERZA] [Top][Summary][Explanatory notes]

1.4.3 [SECP-03] Audit settings

The check verifies if the configuration of the system security audit meets the minimum defined by parameters. The check is designed to test the audit settings by subcategories, which are supported on Windows 6.x (ie. Windows Vista and higher). Category-based settings used on older systems is not verified.

Check result: FAIL.

The use of Group policy is recommended to modify audit settings. The GPO settings path is *Computer Configuration(/Policies)/Windows Settings/Security Settings/Advanced Audit Policy Configuration*.

Note: Although the audit subcategories are supported on Windows 6.0 (ie. Windows Vista and Windows Server 2008), these systems do not support audit subcategory management through Group Policy. Subcategory-based audit settings on these systems can only be changed locally using command line utility *auditpol* or using third-party solutions. Group Policy support is implemented only in Windows 6.1 systems (Windows 7, Windows Server 2008/R2) and higher.

Current audit settings are listed in the table. Subcategories with the audit level lower than required are marked in red.

Category	Subcategory	Value	Recommendation
Account Logon	Credential Validation	Success, Failure	
	Kerberos Authentication Service	Success, Failure	
	Kerberos Service Ticket Operations	Success, Failure	
	Other Account Logon Events	Success, Failure	
Account Management	Application Group Management	Success, Failure	
	Computer Account Management	Success, Failure	
	Distribution Group Management	Success, Failure	
	Other Account Management Events	Success, Failure	
	Security Group Management	Success, Failure	
	User Account Management	Success, Failure	
Detailed Tracking	DPAPI Activity	Failure	

Category	Subcategory	Value	Recommendation
	Process Creation	Failure	☹ min. Success
	Process Termination	Failure	
	RPC Events	Failure	
DS Access	Detailed Directory Service Replication	No auditing	
	Directory Service Access	Success	
	Directory Service Changes	No auditing	
	Directory Service Replication	No auditing	
Logon/Logoff	Account Lockout	Success, Failure	
	IPsec Extended Mode	Success, Failure	
	IPsec Main Mode	Success, Failure	
	IPsec Quick Mode	Success, Failure	
	Logoff	Success, Failure	
	Logon	Success, Failure	
	Network Policy Server	Success, Failure	
	Other Logon/Logoff Events	Success, Failure	
	Special Logon	Success, Failure	
	User / Device Claims	Success, Failure	
Object Access	Application Generated	No auditing	
	Central Access Policy Staging	No auditing	
	Certification Services	No auditing	
	Detailed File Share	No auditing	
	File Share	No auditing	
	File System	No auditing	☹ min. Failure
	Filtering Platform Connection	No auditing	
	Filtering Platform Packet Drop	No auditing	
	Handle Manipulation	No auditing	
	Kernel Object	No auditing	
	Other Object Access Events	No auditing	
	Registry	No auditing	☹ min. Failure
	Removable Storage	No auditing	☹ Success + Failure
	SAM	No auditing	
Policy Change	Audit Policy Change	Success, Failure	
	Authentication Policy Change	Success, Failure	
	Authorization Policy Change	Success, Failure	
	Filtering Platform Policy Change	Success, Failure	
	MPSSVC Rule-Level Policy Change	Success, Failure	
	Other Policy Change Events	Success, Failure	
Privilege Use	Non Sensitive Privilege Use	Failure	
	Other Privilege Use Events	Failure	
	Sensitive Privilege Use	Failure	Success + Failure
System	IPsec Driver	Failure	☹ Success + Failure
	Other System Events	Failure	
	Security State Change	Failure	Success + Failure
	Security System Extension	Failure	Success + Failure
	System Integrity	Failure	Success + Failure

[Computer ERZA] [Top][Summary][Explanatory notes]

1.4.4 [SECP-04] Parameters of log files

Check performs validation of log files parameters. The check is only successful when all three standard logs (application, system, security) are rewritten as needed, their files are stored in the system directory subtree, and the minimal size of each log and its recording time window complies with the check parameters. Furthermore, the guest access to event logs is required to be disabled for systems older than Windows 2003, and the total size of all the logs should not exceed 300 MB for systems older than Windows Vista.

Check result: OK.

These settings can be modified locally, by changing the relevant parameters in the properties of the EventLog using application (mmc snap-in) *Event Viewer*. But in the case of domain computers we rather recommend using Group Policy object (the path to the relevant settings in the GPO is *Computer Configuration(/Policies)/Windows Settings/Security Settings/Event Log*); however, this option is not available in the local GP object (eg. standalone machines).

Log	Parameter	Value	Recommendation
Application	Filename	%SystemRoot %\system32\winevt\Logs\Application.evtx	
	Retention	Overwrite as needed	
	Log size	20.0 MB	
Security	Filename	%SystemRoot %\System32\winevt\Logs\Security.evtx	
	Retention	Overwrite as needed	
	Log size	60.0 MB	
System	Filename	%SystemRoot %\system32\winevt\Logs\System.evtx	
	Retention	Overwrite as needed	
	Log size	20.0 MB	

[Computer ERZA] [Top][Summary][Explanatory notes]

1.4.5 [SECP-05] Other security settings

Check verifies various security parameters of the system not included in other chapters. It is checked whether the Autorun is disabled and if the Windows Error Reporting is disabled; also, correct processing of the Group Policy is verified on domain members.

Check result: FAIL.

Errors in Group Policy objects application are usually due to inadequate configuration of the system components or due to problems at the infrastructure level (server is inaccessible due to the filtration on network elements, permissions do not allow access to network share, etc.). The solution is therefore usually more complicated; system event log may be helpful under some circumstances.

Autorun can be disabled either locally or through an Group Policy object (the GPO setting path is *Computer Configuration/Administrative Templates/System* [Win2003], or *Computer Configuration(/Policies)/Administrative Templates/Windows Components/AutoPlay Policies* [Vista+]) (related link: Autorun and autologon).

Windows Error Reporting can be disabled either locally or through an Group Policy object (the GPO setting path is *Computer Configuration/Administrative Templates/System/Internet Communication Management/Internet Communication settings* [Win2003], or *Computer Configuration(/Policies)/Administrative Templates/Windows Components/Windows Error Reporting* [Vista+]) (related link: Error reporting).

The values to be verified are listed in the table below. Problematic values are marked in red:

Parameter	Value	Recommendation
GP processing	Ok	
Autorun	Disabled	
Wake lock	Enabled in all power modes (locally)	
Screen lock	Disabled (for computer) (settings insufficient in all 3 user profiles)	enable (no more than 900 s)
Windows Defender: Cloud-based protection	Enabled (by default)	disable
Windows Defender: Sample submission	Disabled (locally)	

[Computer ERZA] [Top][Summary][Explanatory notes]

1.5 [USER-xx] User accounts

1.5.1 [USER-01] System-wide privileges

The check verifies that the specified system privileges are not held by anybody outside the defined range of allowable holders. If there is a privilege held by unauthorized user or group, the overall outcome of the check is **FAIL**. Privilege holders are listed in the results table.

Check result: FAIL.

The unauthorized privilege holders can basically only be removed by using Group Policy (if we do not consider third party tools or eg. utilities from the Resource Kit). GPO path to the appropriate settings is *Computer Configuration(/Policies)/Windows Settings/Security Settings/Local Policies/User Rights Assignment*.

The table shows the privilege holders. Conflicting privilege assignments are marked in red:

Privilege	Holder(s)	Recommendation
Access Credential Manager as a trusted caller (SeTrustedCredManAccessPrivilege)		
Act as part of the operating system (SeTcbPrivilege)		
Allow log on locally (SeInteractiveLogonRight)	ERZA\Administrators	
Allow log on through Remote Desktop Services (SeRemoteInteractiveLogonRight)	ERZA\Administrators, ERZA\Remote Desktop Users	
Back up files and directories (SeBackupPrivilege)	ERZA\Administrators, ERZA\Backup Operators	
Create a token object (SeCreateTokenPrivilege)		
Debug programs (SeDebugPrivilege)	ERZA\Administrators	☹ remove privilege holder(s)
Deny access to this computer from the network (SeDenyNetworkLogonRight)	(not assigned: built-in administrator account, built-in guest account)	☹ assign privilege holder(s)
Deny log on locally (SeDenyInteractiveLogonRight)	(not assigned: built-in guest account)	☹ assign privilege holder(s)
Enable computer and user accounts to be trusted for delegation (SeEnableDelegationPrivilege)		
Force shutdown from a remote system (SeRemoteShutdownPrivilege)	ERZA\Administrators	
Impersonate a client after authentication (SeImpersonatePrivilege)	ERZA\Administrators, ERZA\IIS_IUSRS, ERZA\LOCAL SERVICE, ERZA\NETWORK SERVICE, ERZA\SERVICE	
Load and unload device drivers (SeLoadDriverPrivilege)	ERZA\Administrators	
Manage auditing and security log (SeSecurityPrivilege)	ERZA\Administrators	
Modify an object label (SeRelabelPrivilege)		
Restore files and directories (SeRestorePrivilege)	ERZA\Administrators	
	ERZA\Backup Operators	remove privilege holder(s)
Take ownership of files or other objects (SeTakeOwnershipPrivilege)	ERZA\Administrators	

[Computer ERZA] [Top][Summary][Explanatory notes]

1.5.2 [USER-02] Problematic active accounts

The check inspects security-related attributes of user accounts. The active accounts, for which any of the following conditions are true, are considered risky: an account's password does not expire, an account has a password older than one year, an account has a password older than policy limit, an account's password is empty or weak or it cannot be changed, account is locked, account has expired, account is marked trusted for delegation, account may authenticate without Kerberos pre-authentication, account has password stored under reversible encryption, or an account has not logged in during the last year. Problematic accounts are listed in the results table. Exceptions can be defined by the check parameters if necessary.

Check result: OK.

[Computer ERZA] [Top][Summary][Explanatory notes]

1.5.3 [USER-03] Local groups membership

The check verifies whether groups specified by the parameters contain other than explicitly permitted members. The group membership is not evaluated transitively for the purpose of this inspection.

Check result: FAIL.

The listed group members should be removed from the respective groups. This can be done either by modifying the groups directly on the relevant computer or the Group Policy can be used to enforce group membership (Restricted Groups). The GPO settings path is *Computer Configuration(/Policies)/Windows Settings/Security Settings/Restricted Groups*.

The table lists the groups with unauthorized members and the unauthorized members themselves:

Group	Member(s)	Recommendation
ERZA\Administrators	DCIT\Domain Admins, ERZA\Administrator	
	DCIT\ERZA Admins	remove member(s)
ERZA\Backup Operators		
ERZA\Network Configuration Operators		
ERZA\Power Users		
ERZA\Print Operators		
ERZA\Remote Desktop Users		

[Computer ERZA] [Top][Summary][Explanatory notes]

1.5.4 [USER-04] Logon cache

The check reviews the content of the logon cache. The overall result of the check is **FAIL** if there is password verifier recorded in the cache which belongs to a domain account with permissions outside of the current server/workstation. The logon cache entries are listed in the result table.

Check result: OK.

[Computer ERZA] [Top][Summary][Explanatory notes]

1.6 [ACLS-xx] Access control

1.6.1 [ACLS-01] File system of local drives

The check verifies whether all local disks use NTFS as its filesystem. In the case there exists a local drive that does not meet this condition the overall check result is **FAIL**. The offending drives and their details are given in the results table.

Check result: OK.

Of course, the filesystem type cannot be changed centraly. The drive has to be reformatted directly on the given server/station.

Mount point	Volume label/Size	Filesystem	Recommendation
D:\	DATA / 18625 GB	NTFS	
C:\	OS / 275 GB	NTFS	

[Computer ERZA] [Top][Summary][Explanatory notes]

1.6.2 [ACLS-02] File access permissions

The check verifies access permissions (ACLs) of important files and directories. For the successful outcome of the check there may be no file with non-std. owner, no file may have null DACL, and no file may be writable by unprivileged users. Exceptions can be defined by the check parameters if necessary. Files and folders not satisfying the above rules are listed in the results table together with the detailed problem specification.

Check result: OK.

[Computer ERZA] [Top][Summary][Explanatory notes]

1.7 [NETW-xx] Network settings

1.7.1 [NETW-01] Global settings

The check verifies the setting of basic network parameters. For the check to be successful the following conditions must be true: NetBIOS has to be disabled on all network interfaces, IP routing has to be disabled, built-in firewall has to be enabled and system configuration files hosts a lmhosts.sam have to be empty (each of these tests can be disabled by the check parameters if necessary).

Check result: OK WITH WARNING.

These settings (except for the built-in firewall configuration) cannot be managed centrally using Group Policy; values have to be set manually on each server/workstation. The GPO path for Windows built-in firewall settings is *Computer Configuration(/Policies)/Administrative Templates/Network/Network Connections/Windows Firewall*.

Related links:

- Disabling NetBIOS
- Hosts and lmhosts.sam files

The values to be verified are listed in the table below. Problematic values are marked in red:

Parameter	Value	Recommendation
NetBIOS	Disabled	
Installed firewall software	(Windows built-in firewall)	
Current firewall status	Enabled	
IP Routing	Disabled	
System 'hosts' file	Non-empty	☹ verify and possibly remove entries
System 'lmhosts.sam' file	Empty	

[Computer ERZA] [Top][Summary][Explanatory notes]

1.7.2 [NETW-02] Problematic open TCP/UDP ports

Check verifies the open external (not loopback) ports, both TCP and UDP, against the specified set of rules.

Check result: OK WITH WARNING.

Disabling/limiting the accessibility of open ports usually means to stop the service, or to change its configuration (loopback binding), or to filter IP traffic eg. by using the built-in firewall or IPSec filters. It is usually local action that is difficult to centralize (but there are the exceptions - eg. firewall configuration).

Important notice: Windows built-in firewall is enabled on the computer. Its state is not taken into account.

The table lists the blacklisted TCP/UDP ports that are open on external interfaces:

Protocol	Port	Local address	Process	Recommendation
TCP	80	*	4 (System)	☹ limit the access
TCP6	80	*	4 (System)	☹ limit the access
TCP	111	*	2572 (VeeamNFSSvc.exe - VeeamNFSSvc)	
TCP	135	*	964 (svchost.exe - RpcSs)	
TCP6	135	*	964 (svchost.exe - RpcSs)	
TCP	445	*	4 (System)	
TCP6	445	*	4 (System)	
TCP	1063	*	2572 (VeeamNFSSvc.exe - VeeamNFSSvc)	
TCP	1239	*	4 (System)	
TCP6	1239	*	4 (System)	
TCP	1311	*	3656 (dsm_om_connsvc64.exe - Server Administrator)	
TCP6	1311	*	3656 (dsm_om_connsvc64.exe - Server Administrator)	
TCP	1340	*	4 (System)	

Protocol	Port	Local address	Process	Recommendation
TCP6	1340	*	4 (System)	
TCP	2049	*	2572 (VeeamNFSSvc.exe - VeeamNFSSvc)	
TCP	3389	*	3764 (svchost.exe - TermService)	
TCP6	3389	*	3764 (svchost.exe - TermService)	
TCP	5985	*	4 (System)	☹ limit the access
TCP6	5985	*	4 (System)	☹ limit the access
UDP	111	*	2572 (VeeamNFSSvc.exe - VeeamNFSSvc)	
UDP	123	*	928 (svchost.exe - W32Time)	
UDP6	123	*	928 (svchost.exe - W32Time)	
UDP	500	*	640 (svchost.exe - IKEEXT)	
UDP6	500	*	640 (svchost.exe - IKEEXT)	
UDP	1063	*	2572 (VeeamNFSSvc.exe - VeeamNFSSvc)	
UDP	1434	*	696 (sqlbrowser.exe - SQLBrowser)	
UDP6	1434	*	696 (sqlbrowser.exe - SQLBrowser)	
UDP	2049	*	2572 (VeeamNFSSvc.exe - VeeamNFSSvc)	
UDP	3389	*	3764 (svchost.exe - TermService)	
UDP6	3389	*	3764 (svchost.exe - TermService)	
UDP	4500	*	640 (svchost.exe - IKEEXT)	
UDP6	4500	*	640 (svchost.exe - IKEEXT)	

[Computer ERZA] [Top][Summary][Explanatory notes]

1.7.3 [NETW-03] System server components configuration

The check validates some basic parameters of the computer's server components. The two components to be checked are Terminal Server (security level, encryption, in-session password entering) and SNMP service (app-level IP filtering, authentication trap settings and defined communities).

Check result: FAIL.

The configuration of both server components can be done through Group policy; the GPO path to the appropriate settings is *Computer Configuration(/Policies)/Administrative Templates/Network/SNMP* and *Computer Configuration/Administrative Templates/Windows Components/Terminal Services/Encryption and Security* [Win2003], or *Computer Configuration(/Policies)/Administrative Templates/Windows Components/Remote Desktop Services/Remote Desktop Session Host/Security* [Vista+]. However, it should be noted that configuring the SNMP using Group policy can have the security implications, especially as for the definition of the SNMP communities.

The values to be verified are listed in the table below. Problematic values are marked in red:

Service	Parameter	Value	Recommendation
Terminal Server	Allow incomming connections	Enabled	
	Security mode	Full	
	Always require password	Disabled	enable
	Minimum encyption level	High	

[Computer ERZA] [Top][Summary][Explanatory notes]

1.7.4 [NETW-04] Shared resources

The check examines permissions for shared drives. For successful outcome of the check the following conditions have to be true: share has to have std. owner, it has to have non-null DACL, it may not allow access to anonymous users and it may not allow writting to a large non-privileged group (*Everyone*, *Authenticated Users*, *Users*, *Domain Users*) at both the share and the file system level (however, file system permissions check is performed only for the top-level directory of sharing). Exceptions can be specified by check parameters if necessary.

Check result: OK.

Changing sharing parameters and/or permissions is usually highly individual, and it is therefore necessary to perform it locally, directly on the particular server or workstation.

Share	Directory	Problem(s): share	Problem(s): filesystem
print$	C:\Windows\system32\spool\drivers	ok	ok
temp	D:\temp	ok	ok
VBRCatalog	D:\Veeam\VBRCatalog	ok	ok

[Computer ERZA] [Top][Summary][Explanatory notes]

2 EXPLANATORY NOTES

2.1 Classification of findings in results tables

Informational line, no finding.	(no recommendation)
Assessed parameter line, no finding (ok).	(no recommendation)
Assessed parameter line, lower severity finding (warning).	☹ text of recommendation
Assessed parameter line, important finding (error).	text of recommendation

2.2 Abbreviations used

Services access permissions

Null DACL	NULL DACL (no access restriction)
Owner	Owned by non-std. privileged group
ChgCfgACE	Non-std. privileged group can change service config
ExecACE	Anonymous can start/stop service

Security descriptor, the general structure

SD	Security descriptor
D:	Discretionary access list (DACL)
O:	Owner

Security descriptor, ACL flags

P	Protected
AR	Inheritance required
AI	Inherited

Security descriptor, ACE type

A	Allow
D	Deny
U	Audit
M	Mandatory label
OA	Object Allow
OD	Object Deny
OU	Object Audit

Security descriptor, ACE flags

CI	Container inherit
OI	Object inherit
IO	Inherit only
NP	Not propagate
ID	Inherited
SA	Success audit (SACL only)
FA	Failure audit (SACL only)

Security descriptor, ACE permissions

FC	Full control (cumulative)
WR	Write (cumulative)
RD	Read (cumulative)
EX	Execute (cumulative)
[Gfc]	Full control (generic)
[Gwr]	Write (generic)
[Grd]	Read (generic)
[Gex]	Execute (generic)

[Delete]	Delete (standard)
[Read_Ctrl]	Read control (standard)
[Write_DAC]	Write DACL (standard)
[Write_Owner]	Write owner (standard)
[Sync]	Synchronize (standard)
[SACL]	Access SACL (standard)

Security descriptor, permission holders (well-known security principals)

AN	Anonymous logon user
AO	Account operators
AU	Authenticated users
BA	Builtin (local) administrators
BG	Builtin (local) guests
BO	Backup operators
BU	Builtin (local) users
CG	Creator group
CO	Creator owner
ED	Enterprise domain controllers
HI	High mandatory level
IS	IUser
IU	Interactive logon user
LS	Local service
LU	Performance Log users
LW	Low mandatory level
ME	Medium mandatory level
MU	Performance Monitor users
mAA	Windows Authorization Access Group
mBL	Batch logon user
mCS	Creator group server
mDA	Digest Authentication
mDL	Dialup logon user
mNA	NTLM Authentication
mOO	Other Organization
mPX	Proxy
mRL	Remote logon
mSA	SChannel Authentication
mTB	Incoming Forest Trust Builders
mTL	Terminal Server License Servers
mTO	This organization
mTS	Terminal Server
NO	Network configuration operators (to manage configuration of networking features)
NS	Network service
NU	Nework logon user
PO	Printer operators
PS	Personal self
PU	Power users
RC	Restricted code
RD	Remote desktop users (for TS)
RE	Replicator
RU	Pre-windows 2000 compatible group
SI	System mandatory level
SO	Server operators
SU	Service logon user
SY	Local system
WD	Everyone (World)